FMI 3-34.119/MCIP 3-17.01

IMPROVISED EXPLOSIVE DEVICE DEFEAT

September 2005

Expires September 2007

HEADQUARTERS, DEPARTMENT OF THE ARMY
UNITED STATES MARINE CORPS

Foreword

Attacks from improvised explosive devices (IEDs) are one of the major causes of Soldiers and Marines being killed in action (KIA) and wounded in action (WIA). The construct of IED defeat operations supports the National Security Strategy to defeat terrorism and prevent attacks against the United States (U.S.) and coalition forces. It also supports Joint Vision 2020 and the Army Campaign Plan. A key component is the implementation of an integrated IED strategy to counter IED threats and support the Global War on Terrorism. Attaining this goal requires the steady infusion of integrated doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) solutions to counter IED threats to meet the Army's requirements. The IED threat and the protection of our Soldiers and Marines are an extremely important mission. Until recently, there was no single proponent designated to coordinate DOTMLPF solutions for these types of explosive hazards impacting our freedom of maneuver.

In August 2004, the Department of the Army (DA) assigned the United States Army Training and Doctrine Command (TRADOC) as the Army specified proponent for IED defeat. TRADOC then assigned the Maneuver Support Center (MANSCEN) to conduct a mission analysis and determine resource requirements for implementing an integrated DOTMLPF strategy to counter IED threats. MANSCEN was further tasked to establish an IED Defeat Integrated Capabilities Development Team (ICDT) to develop an integrated DOTMLPF strategy to counter IED threats.

This IED Defeat ICDT will interface with the Joint Improvised Explosive Device Defeat (JIEDD) Task Force (TF), and primarily the IED Defeat Joint Integrated Product Team (JIPT), to provide DOTMLPF analysis and assign the appropriate proponency through the process as necessary. The ICDT will also identify and resolve the remaining capability gaps and is tasked with the development, writing, and publication of this field manual interim (FMI) on IED defeat operations.

FMI 3-34.119/Marine Corps Information Publication (MCIP) 3-17.01 is a new FMI publication based on the contemporary operational environment (COE) and emerging tactics, techniques, and procedures (TTP). The emergence of enemy use of IEDs as a preferred method of asymmetric attack, coupled with a strong demand from the field for doctrine to address IED defeat, mandates the development of new doctrine. This manual will serve as a reference for force commanders and staff, training developers, and doctrine developers throughout the Army. Take time to review the materials in this publication and incorporate the doctrine and TTP into your daily operations. The information contained in these pages is useful to all service members regardless of rank.

RANDAL R. CASTRO
MAJOR GENERAL, U.S. ARMY
COMMANDING

This publication is available at

Army Knowledge Online

www.us.army.mil

Field Manual Interim
No. 3-34.119
Marine Corps Information Publication
No. 3-17.01

Headquarters,
Department of the Army
United States Marine Corps
Washington, DC, 21 September 2005
Expires 21 September 2007

IMPROVISED EXPLOSIVE DEVICE DEFEAT

Contents

Preface

FMI 3-34.119/MCIP 3-17.01 establishes doctrine (fundamental principals and TTP) for the defeat of adversary IED operations. It is based on existing doctrine and lessons learned from recent combat operations.

This publication applies to the Active Army, the Army National Guard (ARNG)/the Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR). The primary audience for this FMI is commanders, leaders, and staffs at corps-level and below.

To make this manual useful to leaders involved in IED defeat operations regardless of where these operations may occur, the doctrine contained herein is broad in scope and involves principles applicable to various theaters. This FMI is not focused on any region or country. IED operations have some common characteristics, but their methods of implementation may vary widely.

FMI 3-34.119/MCIP 3-17.01 is not a stand-alone document. Readers must be familiar with the fundamentals of assured mobility found in Field Manual (FM) 3-34. This manual uses assured mobility as a framework to assist leaders with planning and executing IED defeat operations. Additionally, this FMI incorporates lessons learned and major studies from sources across the Army and joint community. It focuses on the asymmetric threats and establishes doctrine to defeat those threats.

Note. An FMI is a DA publication that provides expedited delivery of urgently needed doctrine that the proponent has approved for use without placing it through the standard development process. Unless an FMI is rescinded, the information it disseminates is incorporated into a new or revised FM. An FMI expires after two years, unless superseded or rescinded.

This manual—

- Provides doctrinal guidance for commanders and staffs for planning, preparing for, and executing and assessing IED defeat operations.
- Serves as an authoritative reference for emerging doctrine, TTP, materiel and force structure, institutional and unit training, and standing operating procedures (SOPs) for IED defeat operations.
- Outlines the critical roles and responsibilities of staff cells for IED defeat operations.

Terms that have joint or Army definitions are identified in both the glossary and the text. Glossary references: The glossary lists most terms used in FMI 3-34.119/MCIP 3-17.01 that have joint or Army definitions. Terms for which FMI 3-34.119/MCIP 3-17.01 is the proponent FMI (the authority) are indicated with an asterisk in the glossary. Text references: Definitions for which FMI 3-34.119/MCIP 3-17.01 is the proponent FMI are printed in boldface in the text. These terms and their definitions will be incorporated into the next revision of FM 1-02. For other definitions in the text, the term is italicized and the number of the proponent FM follows the definition.

The proponent for this publication is United States Army Training and Doctrine Command. The preparing agency is the Doctrine Development Division, United States Army Engineer School. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commandant, United States Army Engineer School, ATTN: ATSE-DD, Suite 336, 320 MANSCEN Loop, Fort Leonard Wood, Missouri 65473-8929.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Introduction

"This is not a new war. Our enemies have been waging it for some time, and it will continue for the foreseeable future. As President Bush has stated, 'This is a different kind of war against a different kind of enemy.' It is a war we must win, a war for our very way of life."

General Peter J. Schoomaker,
Chief of Staff of the Army
Arrival Message, 1 August 2003

The proliferation of IEDs on the battlefield in both Iraq and Afghanistan has posed the most pervasive threat facing coalition forces in those theaters. The persistent effectiveness of this threat has influenced unit operations, U.S. policy, and public perception. IEDs are a weapon of choice and are likely to remain a major component of the Global War on Terrorism for the foreseeable future.

The definitive history of IEDs has not been extensively documented. However, many specific incidents in the last 100 years have been well documented. Recently there has been a trend of increasing terrorist acts against the United States. These attacks have increased in their frequency, in their level of sophistication, and in their lethality. For example, the Marine barracks in Beirut, Lebanon, was attacked with a truck bomb that killed 241 U.S. Marines in 1983. This was followed by the bombing of Pan American Flight 103 over Lockerbie, Scotland, in 1988. (The plane carried passengers from 21 countries, but 189 of the 259 on board were Americans; the crash also killed 11 people on the ground.) In the first terrorist attack on the World Trade Center in New York City in 1993, a truck bomb failed to cause the desired number of casualties but nevertheless demonstrated the ability to attack the U.S. homeland. In 1996, another truck bomb killed 19 U.S. Soldiers and injured 372 at the Khobar Towers housing complex in Dhahran, Saudi Arabia. The violence continued with the bombings of the United States embassies in Kenya and Tanzania in 1998 and the United States Ship (USS) Cole in the port of Aden, Yemen, in 2000.

With the development of sufficiently powerful, stable, and accessible explosives, a preferred weapon of a terrorist is a bomb or IED. As a weapon, bombs are efficient as they allow a person or group to strike with great destructive effect. The sophistication of the device depends on the maker. They can range from being very simple to very complex with booby traps, antihandling devices, and sophisticated electronic initiation devices to prevent disarming. Generally, bombs can be triggered in a variety of ways. A timer is common and can be set hours in advance. Remote-controlled detonators with a limited range allow the timing of the detonation exactly. Bombs can be manufactured out of many household products (including fertilizer and batteries), but most sophisticated bombs use a small amount of explosive to trigger a larger quantity of poorer grade explosive material. Bombs do not have to be large to be effective. Most bombs are small and are directed at individual targets, such as military personnel or politicians. Often these are planted along a roadside and detonated as a vehicle passes. Larger devices can be placed in vehicles parked along the roadway or driven into the target by suicide bombers willing to give up their lives for the cause.

This manual provides commanders, leaders, and staffs with fundamental principals and TTP for the defeat of adversary IED operations. Based on current doctrine, this manual also incorporates the lessons learned from recent combat operations. The following briefly describes the chapters and appendixes:

- Chapter 1 defines IED defeat operations. It describes how commanders and their staff use the IED defeat framework to assist with planning, preparing, executing, and assessing IED operations.
- Chapter 2 provides a description of the COE in which IEDs are employed. It explains how and why the enemy uses IEDs to disrupt friendly operations from a strategic to a tactical perspective.
- Chapter 3 defines how threat forces operate and how they use IEDs.

- Chapter 4 provides the characteristics of IEDs and offers threat TTP on their use and employment. It describes the components and common initiation methods. It also provides basic indicators and locations of where IEDs can be used.
- Chapter 5 identifies U.S. government agencies that are involved in IED defeat operations. It is not an all-inclusive list. It covers agencies from the strategic level to the operational level and includes intelligence and technology development organizations. This chapter provides basic mission statements of the organizations.
- Chapter 6 provides guidance for a leader upon encountering an IED. All units must be able to maintain operations despite these hazards. It briefly describes military search and route clearance operations.
- Chapter 7 provides an overview of the planning processes of the Army and describes how a commander and his staff integrate IED defeat considerations into unit plans. Additionally, it discusses intelligence preparation of the battlefield (IPB), targeting, and risk management as additional tools to assist the commander and staff in integrating IED defeat considerations throughout. This chapter also offers planning considerations for IED defeat based on the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). The METT-TC factors are not all-inclusive but serve as a base for further development depending on the situation.
- Chapter 8 provides information to develop a training strategy for preparing units for IED defeat operations.
- Appendix A complies with current Army directives which state that the metric system will be incorporated into all new publications.
- Appendixes B through H provide greater depth to the chapters and offer basic suggestions for conducting IED defeat operations.

Chapter 1
Fundamentals

With the proliferation of technology and access to explosive materials, many enemy groups have come to rely on IEDs as a primary means of attack. As seen in recent conflicts in Afghanistan and Iraq, IED attacks have destabilizing and destructive effects on friendly operations. This chapter defines IED defeat operations and provides commanders, leaders, and staffs with a framework to effectively counter-IED attacks. Additionally, this chapter provides key definitions associated with IED defeat.

SECTION I – OPERATIONS

1-1. The focus of IED defeat is often on the IED itself. However, the device is merely the end product of a complex set of enemy activities. An IED attack is the result of a planned tactical operation with several key elements that work in a coordinated and synchronized manner to attain a desired result. The results can have operational or strategic impacts, not solely because of the military value of the target, but also the psychological impact on units, the local population, the world community, and political leaders.

1-2. Successful IED defeat operations begin with a thorough understanding of the enemy and the common activities associated with an IED attack. Activities include leadership, planning, financing, materiel procurement, bomb making, target selection, recruiting, and attack execution. A holistic approach to understanding the requirements of an IED attack assists commanders and planners in identifying vulnerabilities. These vulnerabilities can be exploited to break the operational chain of events of the enemy. See Chapter 3 for a detailed discussion on enemy IED attack characteristics.

1-3. IED defeat operations are unit activities that are planned, prepared for, executed, and assessed to identify, deter, and mitigate the effects of an IED attack. As part of the broader mission of the unit, these activities are conducted to predict, detect, prevent, avoid, neutralize, and protect the force from IED attack. IED defeat operations are not a staff- or function-specific responsibility. IED defeat cuts across the battlefield operating systems (BOS) and requires the entire staff to consider all options to eliminate the IED threat. The goal is to identify and defeat enemy leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs, while protecting the force from the effects of an IED attack.

SECTION II – FRAMEWORK

1-4. The IED defeat framework derives from the imperatives and fundamentals of assured mobility that are found in FM 3-34. Assured mobility encompasses those actions that enable commanders with the ability to deploy, move, and maneuver where and when they desire (without interruption or delay) and to achieve the mission (see FM 3-34).

1-5. The IED defeat framework is a parallel construct to assured mobility and enables commanders and staffs to plan and take proactive measures to seek out and defeat IED events before they occur. It also provides a methodology for addressing IED events upon contact and subsequent detonation. The IED defeat framework (Figure 1-1, page 1-4) consists of the following:

- **Predict activities.** These activities are used to identify and understand enemy personnel, equipment, infrastructure, TTP, support mechanisms, or other actions to forecast specific enemy IED operations directed against U.S. interests. This is driven largely by success in analysis in the requirements management. Predict activities assists in—
  - Identifying patterns of enemy behavior.
  - Identifying emerging threats.
  - Predicting future enemy actions.
  - Prioritizing intelligence, surveillance, and reconnaissance (ISR) missions.
  - Exploiting IED threat vulnerabilities.
  - Targeting enemy IED attack nodes (such as funding and supplies).
  - Disseminating alert information rapidly to specific users.
  - Analyzing forensics and enabling better on-scene technical analysis.
- **Detect activities.** These activities contribute to the identification and location of enemy personnel, explosive devices, and their component parts, equipment, logistics operations, and infrastructure in order to provide accurate and timely information. These actions assist in the efforts to interdict and destroy these activities. Detect activities aid in—
  - Detecting and identifying explosive material and other IED components.
  - Detecting chemical, biological, radiological, and nuclear (CBRN) material.
  - Recognizing suicide bombers.
  - Conducting forensic operations to track bomb makers and/or handlers.
  - Conducting persistent surveillance.
  - Training to improve detection of IED indicators by digital means.
  - Developing priority information requirements (PIR) tied to IED operations decisive points. Linking and synchronizing detection assets to PIR-related named areas of interest (NAIs).
  - Using detection means across the full range available (from imagery, mechanical-clearance operations, search techniques, dogs, and so forth).
  - Recognizing individual Soldier actions and awareness in all activities.
- **Prevent activities.** These activities disrupt and defeat the IED operational chain of events. The actions focus on the target to interdict or destroy key enemy personnel (bomb makers, leaders, and financiers), the infrastructure/logistics capabilities (suppliers and bomb factories), and surveillance/targeting efforts (reconnaissance and overmatch operations) before emplacement of the device. They also include actions to deter public support for the use of IEDs by the enemy. Prevent activities aid in—
  - Disrupting enemy operations and their support structure.
  - Denying critical IED-related supplies to the enemy.
  - Increasing awareness of enemy TTP and their effectiveness.
  - Denying the enemy the opportunity to emplace IEDs (through presence patrols, observation posts, checkpoints, aggressive surveillance operations, and so forth).
  - Rewarding local nationals' cooperation in determining the locations of caches, bomb making, or emplacing activities.
  - Denying easily concealed locations (such as trash piles and debris along sides of primary routes) and removing abandoned vehicles along routes.

- **Avoid activities.** These activities keep friendly forces from IEDs when prevention activities are not possible or have failed. Avoid activities include—
  - Increasing situational understanding (SU) of the area of operations (AOs) and continually refining the common operational picture (COP) and the timely and accurate dissemination of related information.
  - Ensuring timely and accurate status reporting and tracking.
  - Altering routes and routines.
  - Marking and bypassing suspected IEDs.
- **Neutralize activities.** These activities contribute to the destruction or reduction of enemy personnel, explosive devices, or supplies. They can be proactive or reactive in nature.
  - Proactive activities include conducting operations to eliminate or interrupt the enemy's leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs against coalition forces.
  - Reactive activities include conducting controlled detonations or render safe procedures (RSPs) against identified IEDs, caches, captured enemy ammunition (CEA), and so forth. Explosive ordnance disposal (EOD) forces are the only personnel authorized to render safe IEDs.
- **Protect activities.** These activities improve the survivability of IED targets through hardening, awareness training, or other techniques. Protect activities include—
  - Disrupting, channeling, blocking, or redirecting energy and fragmentation.
  - Creating greater standoff distances to reduce the effect that IEDs have on their intended targets.
  - Incorporating unmanned platforms.
  - Using jamming devices.
  - Reducing time and distance in which intended targets are within IED range.
  - Accelerating processes and increasing the effectiveness by which reaction and evacuation operations are conducted.
  - Providing blast and fragmentation mitigation for platforms, structures, and personnel.
  - Avoiding establishing patterns and predictable forms of behavior.
  - Conducting proper precombat inspections (PCIs) and rehearsals for all operations.
  - Treating every operation as a combat mission (from a simple convoy to daily forward operating base [FOB] security).

1-6. The IED defeat framework (Figure 1-1, page 1-4) can be broken down into two major subelements—proactive (predetection) and reactive (postdetection).

- Proactive elements are actions taken by friendly forces to predict, detect, prevent, avoid, neutralize, and protect against IED events.
- Reactive elements are actions taken by friendly forces to detect, avoid, neutralize, and protect against IED events.

Note. The fundamentals of detect, avoid, neutralize, and protect applies to both sides of the framework (proactive and reactive measures).

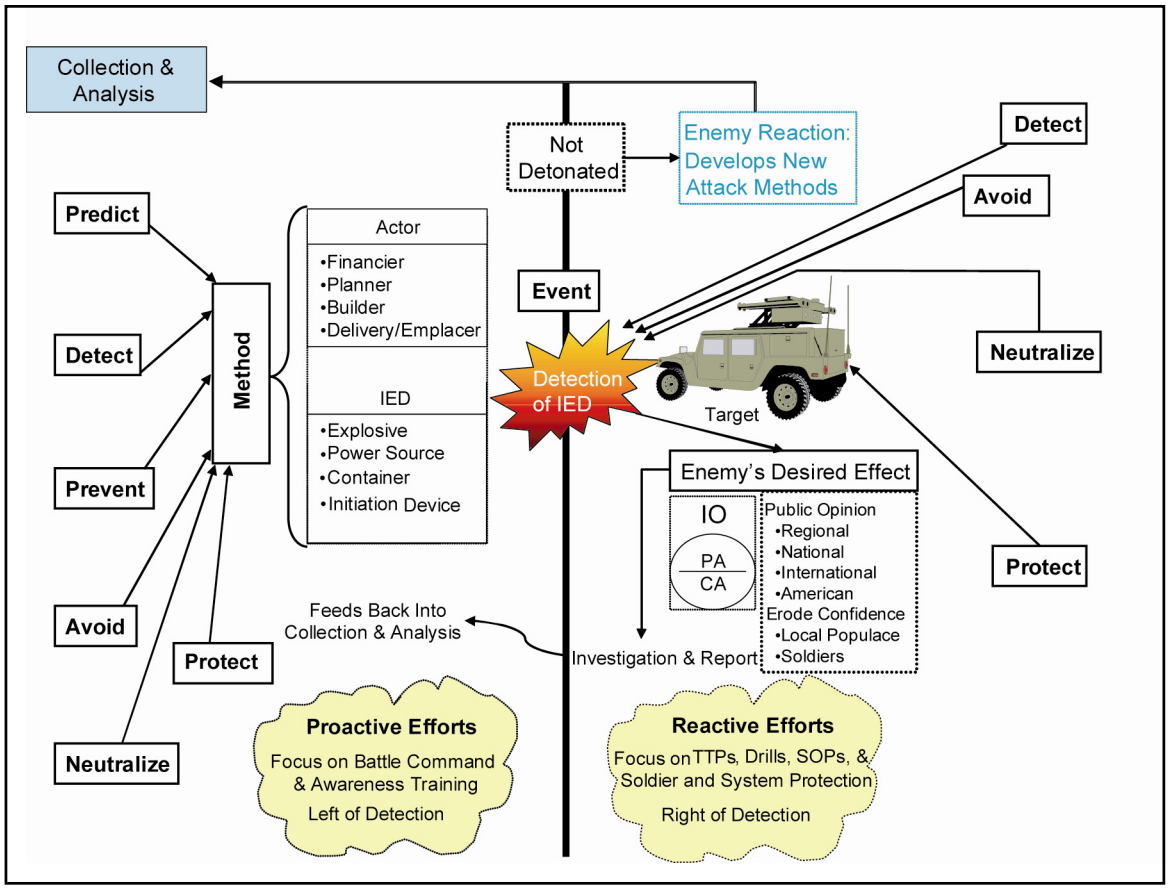

Figure 1-1. IED defeat framework

SECTION III – TERMINOLOGY

1-7. The following terminology is inherent to IED defeat and is used throughout this manual:

- **Booby trap.** A *booby trap* is an explosive or nonexplosive device or other material deliberately placed to cause casualties when an apparently harmless object is disturbed or a normally safe act is performed (Joint Publication [JP] 1-02).
- **Captured enemy ammunition.** A *CEA* is all ammunition products and components produced for or used by a foreign force that is hostile to the United States (that is or was engaged in combat against the United States) in the custody of a U.S. military force or under the control of a Department of Defense (DOD) component. The term includes confined gaseous, liquid, and solid propellants; explosives; pyrotechnics; chemical and riot-control agents; smokes and incendiaries (including bulk explosives); chemical warfare agents; chemical munitions; rockets; guided and ballistic missiles; bombs; warheads; mortar rounds; artillery ammunition; small arms ammunition; grenades; mines; torpedoes; depth charges; cluster munitions and dispensers; demolition charges, and devices and components of the above. CEA can also include North Atlantic Treaty Organization (NATO) or U.S. manufactured munitions that may not have been under U.S. custody or control.
- **Defeat.** *Defeat* is a tactical mission task that occurs when an enemy force has temporarily or permanently lost the physical means or the will to fight. The defeated force's commander is unwilling or unable to pursue his adopted course of action (COA), thereby yielding to the friendly commander's will, and can no longer interfere to a significant degree with the actions of friendly forces. Defeat can result from the use of force or the threat of its use (FM 1-02).

- **Explosive hazard. An *explosive hazard* is any hazard containing an explosive component. All explosive hazards currently encountered on the battlefield can be broken down into five categories: unexploded ordnance (UXO), booby traps, IEDs, CEA, and bulk explosives.**
- **Explosive ordnance.** *Explosive ordnance* is all munitions containing explosives, nuclear fission or fusion materials, and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket, and small arms ammunition; all mines, torpedoes, and depth charges; demolition charges; pyrotechnics; clusters and dispensers; cartridge and propellant-actuated devices; electro-explosive devices; clandestine and IEDs; and all similar or related items or components explosive in nature (JP 1-02).
- **Improvised explosive device.** An *IED* is a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. Also called IED (JP 1-02).
- **Improvised explosive device hunting. *Improvised explosive device hunting* is a counter-IED operation to proactively locate IEDs and the personnel who make and emplace them before the IED is detonated. See also military search.**
- **Military search. *Military search* is the management and application of systematic procedures and appropriate detection equipment to locate specified targets.**
- **Neutralize.** The definition of *neutralize* is used—1. As pertains to military operations, to render ineffective or unusable. 2. To render enemy personnel or material incapable of interfering with a particular operation. 3. To render safe mines, bombs, missiles, and booby traps. 4. To make harmless anything contaminated with a chemical agent (JP 1-02).
- **Render-safe procedures.** *Render-safe procedures* are to render safe those particular courses or modes of action taken by EOD personnel for access to, diagnosis, rendering safe, recovery, and final disposal of explosive ordnance or any hazardous material associated with an EOD incident. The RSPs include the portion of the EOD procedures involving the application of special EOD methods and tools to provide for the interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation (JP 1-02).
- **Unexploded explosive ordnance; unexploded explosive.** *Unexploded explosive ordnance/unexploded explosive* is explosive ordnance which has been primed, fused, armed, or otherwise prepared for action, and which has been fired, dropped, launched, projected, or placed in such a manner as to constitute a hazard to operations, installations, personnel, or material and remains unexploded either by malfunction or design or for any other cause. Also called UXO (JP 1-02).

This page is intentionally left blank.

Chapter 2

Contemporary Operational Environment

The persistent effectiveness of the IED threat has impacted unit operations, U.S. policy, and public perception. Therefore, this deadly enemy capability is likely to be a component of war and armed conflict for the foreseeable future. This chapter provides an overview of the COE and the baseline rationale for why and how state and nonstate actors employ IEDs against a superior military force. In the complicated environment of today, it is impossible to predict the exact nature of the operational environment (OE) in which IEDs might be used. Therefore, the U.S. Army must be ready to meet challenges that IEDs present within a multitude of diverse OEs. The FM 7-100 series manuals introduce the baseline for the COE and should be referred to in conjunction with this manual when training against a nonspecific capabilities-based enemy operating in an environment that is adaptive and asymmetrical.

CONCEPT

2-1. *OE* is defined as a composite of the conditions, circumstances, and influences that affect the employment of military force and bear on the decisions of the unit commander (JP 1-02). The OE is complex, dynamic, multidimensional, and comprises a collection of interrelated variables.

2-2. The COE is the synergistic combination of all the critical variables that represent the conditions, circumstances, and influences that can affect military operations today and for the foreseeable future. The COE concept can be used to describe the overall global OE or the manifestations of this OE in one or more specific OEs that exist within it. Finally, the COE concept provides a conceptual framework for assessing and understanding the nature of any specific OE. Therefore, the conceptual framework for understanding a specific OE and why the enemy uses IEDs must include an analysis of the critical variables of the COE.

CRITICAL VARIABLES

2-3. There are a number of variables, including but not limited to military capabilities, that affect the use of IEDs. These are the same critical variables by which the nature of any OE can be defined. As these conditions, circumstances, and influences vary according to the particular situation, so does the exact nature of a specific OE. These variables are interrelated and sometimes overlap. Different variables will be more or less important in different situations, but they are all common to any OE. The most difficult aspect of analyzing the OE is that the content of the variables does not remain fixed, but will evolve overtime. Therefore, we can expect the environments in which we are operating to change overtime. Nevertheless, the collective content of these variables will define any OE in which the Army might encounter IEDs at a given time and place.

2-4. While these variables can be useful in describing the overall (strategic) environment within which IEDs are used, they are most useful in defining the nature of specific OEs. Each OE is different because the content of the variables is different. Only by studying and understanding these variables will the U.S. Army be able to keep adversaries from using them against our forces or to find ways to use them to our own advantage. Beyond the assessment of individual variables, it is crucial to appreciate the relationships that exist among the variables and how this impacts the OE.

2-5. Before examining the types of OE in which IEDs might be employed, from the perspective of each of the eleven COE variables, there are some basic premises that characterize the general nature of the COE. In the foreseeable future, the United States is not likely to have a peer competitor that would be able to

engage U.S. forces head-to-head in conventional combat on a large scale. Nations that believe the United States may intervene in their country or region will develop adaptive approaches for dealing with technologically superior forces. Nonstate actors are now playing and will continue to play an important role in any regional conflict—as combatants or noncombatants. Any specific OE in which we might encounter IEDs is a manifestation of the overall nature of the COE. The following are the eleven COE variables:

- Physical environment.
- Nature and stability of the state or nonstate actors.
- Sociological demographics.
- Regional and global relationships.
- Military and paramilitary capabilities.
- Technology.
- Information.
- External organizations.
- National will or nonstate actors will.
- Time.
- Economics.

PHYSICAL ENVIRONMENT

2-6. The enemy clearly understands that less complex and open environments favor U.S. forces with our long-range, precision-guided weapons and our sophisticated ISR capability. Because of this, the enemy usually avoids open terrain and operates in urban areas and other complex terrain to mitigate U.S. technical superiority. Such terrain is also optimal for emplacing IEDs with minimal risk to those who emplace them. However, the physical environment includes more than just terrain and weather patterns. Natural resources, population centers, and critical infrastructures are also important, especially since they may become targets for IEDs.

Note. Complex terrain is a topographical area consisting of an urban center larger than a village and/or of two or more types of restrictive terrain or environmental conditions occupying the same space. (Restrictive terrain or environmental conditions include, but are not limited to slope, high altitude, forestation, severe weather, and urbanization.) Complex terrain, due to its unique combination of restrictive terrain and environmental conditions, imposes significant limitations on observation, maneuver, fires, and intelligence collection.

NATURE AND STABILITY OF THE STATE OR NONSTATE ACTORS

2-7. In the state or states within which the IEDs are employed, the nature and stability of a country often is related to where the real strength of the state lies. It may be the political leadership, the military, the police, or some other element within the population. In understanding where the power resides, you can analyze who would use IEDs, against whom, and why—as a means to achieve a specific end. Those who employ IEDs may be nonstate actors (such as criminals, insurgents, or terrorists) that are either subnational or transnational in nature; in that case, you need to understand the nature and stability of the nonstate organization. A weak state may be unable to control the activities of nonstate actors who would use IEDs within its territory.

2-8. The enemy can be any individual, group of individuals (organized or not organized), paramilitary or military force, national entity, or national alliance that is in opposition to the United States, its allies, or its multinational partners. In the case of IEDs, the enemy can be any individual, group, or organization that employs IEDs, regardless of their motivation. These adversaries include the people who build the IEDs, those who plan their use, those who emplace them, those who conduct surveillance before and after emplacement, and those who harbor or provide sanctuary to the perpetrators or provide them financial or material support.

SOCIOLOGICAL DEMOGRAPHICS

2-9. The demographics variable includes the cultural, religious, and ethnic makeup of a given region, nation, or nonstate actor. Extreme devotion to a particular cause and/or hatred against another nation or another cultural, religious, or ethnic group provides the enemy with the willingness to carry out IED attacks. This variable can be analyzed to determine how far the enemy would go to carry out his attacks (for example, suicide bombers), who it is likely to attack, and where it is likely to attack (where those hated groups or individuals reside, work, or travel or locations of symbolic value).

2-10. Cultural, religious, or ethnic links can cause the local population to support the enemy, to include providing the enemy with information about possible targets for IEDs. However, by understanding the sociological demographics of the local population, U.S. or coalition forces can address the needs of the people and avoid offending their sensitivities. Winning over the population can be a crucial element in successfully fighting the IED threat. If treated properly, the populace can be cooperative about providing U.S. or coalition forces with information about enemy activity, the location of weapons caches and bomb-making factories, and the locations of emplaced IEDs.

2-11. The aforementioned physical environment is intertwined with our analysis of sociological demographics. For example, an urban environment is affected by the cultures found within it. Since the enemy prefers to operate in complex terrain and the majority of the world population resides in urban settings, the potential for U.S. forces to continue to operate in this type of environment is a reality. The enemy will use IEDs not only to target U.S. forces, but also to target specific groups or individuals within the population (often in an urban setting).

REGIONAL AND GLOBAL RELATIONSHIPS

2-12. The relationship of a state or nonstate actor to other actors and the level of allegiance to that relationship can determine the effectiveness of IEDs in a specific OE. These relationships can determine the level of support and motivation and increase the capability of the enemy to use IEDs. When analyzing the OE, closely consider the relationships that exist between state and nonstate actors and what this means in terms of funding, training, equipping, and manning of forces employing IEDs.

2-13. Regional and global relationships could be between similar kinds of nonstate actors (for example, terrorists) who could share TTP for building and employing IEDs. Nation-states could share these TTP with nonstate actors and vice versa.

MILITARY AND PARAMILITARY CAPABILITIES

2-14. Military capabilities are most often thought of in terms of a standing professional force. However, the enemy does not require a standing army to use IEDs in order to achieve a specific means. When considering the impact of military capabilities on the use of IEDs, more important is the level of equipment, training, resources, and leadership available for procurement, development, and execution of IEDs.

2-15. Paramilitary organizations are those that are distinct from the regular armed forces but resemble them in organization, equipment, training, or purpose. Basically, any organization that accomplishes its purpose, even partially, through the force of arms can be considered a paramilitary organization. Some types of paramilitary organizations (such as police and other internal security forces) may be part of the government infrastructure. Other types (such as insurgents, terrorists, and large-scale drug and other criminal organizations) operate outside the government or any institutionalized controlling authority. When it is expedient for their purposes, these paramilitary forces can employ IEDs.

TECHNOLOGY

2-16. Easy access to new technology allows the enemy to achieve equality or even overmatch U.S. forces in selected niche areas. IEDs range from relatively crude devices to fairly sophisticated and precision weapons. In their own way, IEDs can be precision weapons. Analysis of the technology variable is critical

for maintaining SU and for determining what types of IEDs, methods of emplacement, and triggers the enemy will use.

2-17. Advanced technology is available on the world market for a wide variety of nation-state and nonstate actors who can afford it. However, any of these actors (if their intent is hostile to U.S. interests) will attempt to find ways to use whatever technology is available to them in adaptive and innovative ways against us. For example, the enemy can use readily available communications technology (such as cellular or satellite telephones or handheld radios) to communicate with operatives or to remotely detonate IEDs.

INFORMATION

2-18. The enemy understands the value of information and information warfare (IW). The enemy has seen the important role that IW has played in achieving the overall objectives of various actors in current and past conflicts. Media and other information means facilitate the visibility of IED operations to the world (providing publicity), while the use of IEDs can provide standoff and anonymity to the user. The enemy can use the perception management aspect of IW to try to provide justification for its actions and as a means for recruitment. Knowing that casualties from IEDs will be publicized in the media in the United States and other coalition countries, the enemy can use this reporting to affect the U.S. national will and the coalition will. The enemy will exploit U.S. mistakes and leverage the media and other information systems to impact U.S. political decision making. IW is a nonlethal tool that is used in conjunction with lethal operations to achieve an end.

2-19. The enemy will emphasize the fact that U.S. and coalition forces and/or local authorities are unable to protect themselves or the local population from the effects of IEDs. This is a physical and psychological threat to elements of the local population; it can keep them from supporting U.S. objectives and coerce them into providing aid to enemy forces or at least passively protecting them.

EXTERNAL ORGANIZATIONS

2-20. External organizations (such as international governmental organizations, nongovernmental organizations [NGOs], media, transnational corporations, and private security organizations) impact the enemy's decisions on whom to target, how to target, and how to manipulate the situation for its benefit. External organizations within the OE provide the enemy with a multitude of targets, opportunities for concealment among noncombatants, and potential information gatherers—all of which the enemy can use to its advantage when employing IEDs. Analyzing this variable can help determine where the enemy will use IEDs, who it will target, and how.

NATIONAL WILL OR NONSTATE ACTORS WILL

2-21. The unification of common values within a segment of the population and a unified effort to pursue, protect, and/or spread those values can further the ability of the enemy to achieve its ends. It can also define the level of support the enemy can expect to sustain from the local population and/or other populations sharing those common values. The enemy will attempt to attack the U.S. national will or the coalition partners will through the use of IEDs (along with IW) because they provide a tactical weapon with which to achieve strategic goals. The enemy uses IEDs because it believes they are effective and that the use of IEDs is acceptable at least to the members of the group or cause on whose behalf it is using them.

2-22. Victory does not necessarily go to the best-trained or best-equipped entity but to the entity that is willing to sacrifice the most in order to win. The enemy entity may view the will of its organizational leadership and the devotion and collective will of its members and supporters as an advantage over the United States or a U.S.-led coalition. The will of a suicide bomber may reflect the overall will of the organization that sent him to deliver the IED.

TIME

2-23. In an era of push-button technology and past U.S. successes in relatively short-time periods, the enemy will attempt to prolong U.S. operations for as long as possible until the U.S. national will and/or the coalition will falters. A protracted campaign of IED use can be a means for the enemy to achieve this. The enemy views time as an advantage for itself and not for the United States.

2-24. Ways that IEDs support the enemy's use of time are often at critical junctures, such as when U.S. forces attempt entry into an OE. The enemy will take advantage of the relatively immature and nonsecure sea ports of debarkation (SPODs) and aerial ports of debarkation (APODs) and use IEDs as a weapon of choice.

2-25. Another way in which enemy employment of IEDs may be affected by time would be if the enemy determined that U.S. or coalition forces deployed in the region become less alert to the IED threat over time. If a unit or an area has not been targeted by IEDs for a period of time, complacency and lack of attention may make U.S. or coalition forces more vulnerable targets.

2-26. Over time, the enemy will change the types of IEDs and triggering devices it uses and its TTP for employing them. U.S. or coalition forces may be trained to look for certain things, but when the enemy observes that forces are looking for those things it will adapt by doing something different.

ECONOMICS

2-27. The economic factors differ from one specific OE to another. Differences in the ability to produce, distribute, and receive goods are important to the frequency of IED use and the types of IEDs used. As previously mentioned, IEDs range from relatively crude devices to fairly sophisticated and precision weapons. With IEDs, an enemy can use a large number of cheap, expendable things to affect the ability of the United States to use a limited number of expensive precision munitions or other high-technology systems. The economic situation within an OE should be carefully analyzed to determine what is currently available to the enemy, its ability to acquire materials, the level of sophistication, and its ability to sustain IED operations.

2-28. IEDs can be used to attack economic targets. Sometimes their purpose is not to inflict casualties, but rather to disrupt the flow of goods or resources. IED attacks against critical infrastructures can cripple an economy.

ADAPTIVE PRINCIPLES OF THE ENEMY

2-29. An enemy who is not a peer competitor will avoid engaging U.S. and/or coalition forces in a head-to-head conventional fight. The enemy will not fight U.S. or coalition forces in the same manner as it would its peers or lesser forces in its region. Instead, it will have to resort to adaptive approaches in order to accomplish its goals against a U.S. or coalition force that overmatches it in conventional military power. Asymmetry in warfare is not a new phenomenon, but given the relative capabilities of the United States as opposed to its potential opponents, it is increasingly likely that our enemies will seek adaptive, asymmetric approaches. They will seek to avoid or counter U.S. strengths without having to oppose them directly, while exploiting perceived U.S. weaknesses. In such cases, IEDs may become the weapons of choice.

2-30. Various nation-state and nonstate actors generally view the United States as having an overall advantage in technology and warfighting capability. Despite our strengths, these actors also see some weaknesses that they may be able to exploit. Actions against such a superior force will focus on perceived centers of gravity (such as national will and the willingness to endure casualties, hardship, stress, and continued deployments overtime). Based on these perceived vulnerabilities, enemy forces are likely to employ the following principles for dealing with technologically or numerically superior forces:

- Cause politically unacceptable casualties.
- Control access into the region.
- Employ operational shielding.
- Neutralize technological overmatch.

- Control the tempo.
- Change the nature of the conflict.
- Allow no sanctuary.

CAUSE POLITICALLY UNACCEPTABLE CASUALTIES

2-31. The enemy will attempt to inflict highly-visible and embarrassing losses on U.S. forces in order to weaken U.S. domestic resolve and national will to sustain the deployment or conflict. In recent history, modern wealthy nations have shown an apparent lack of commitment overtime and sensitivity to domestic and world opinion in relation to conflict and seemingly needless casualties. The enemy will try to influence public opinion in the U.S. homeland to the effect that the goal of intervention is not worth the cost.

2-32. IEDs are well-suited to the goal of causing politically unacceptable casualties. They can cause a relatively large number of casualties for a relatively small expense. The casualties do not necessarily have to be within U.S. or coalition forces. The United States or its coalition partners may be even less willing to accept military or civilian casualties.

CONTROL ACCESS INTO THE REGION

2-33. U.S. and coalition forces capable of achieving overmatch against the enemy must first enter the region using power-projection capabilities. To completely deter U.S. or coalition involvement or severely limit its scope and intensity, the enemy would first target the national will of the United States and/or its coalition partners. Given the challenges IED operations have caused for U.S. and coalition forces in the past, an enemy could mount an extensive IED campaign in its region in order to dissuade such forces from intervening there.

2-34. Access-control operations do not necessarily have to deny access entirely. A more realistic goal is to limit the U.S. or coalition accumulation of applicable combat power to a level and to locations that do not threaten the goals of the enemy organization. One means of accomplishing this is the employment of IEDs to attack U.S. or coalition forces at APODs and SPODS, along routes to the region, at transfer points en route, at aerial ports of embarkation (APOEs) and sea ports of embarkation (SPOEs), and even at their home stations. These are fragile and convenient targets. In order to selectively deny a U.S. or coalition force the use of or access to forward bases of operation within or near the region, enemy organizations might use IEDs to attack the population and economic centers for the intimidation effect.

EMPLOY OPERATIONAL SHIELDING

2-35. The enemy will use any means necessary to protect key elements of its forces or infrastructure from destruction by a more powerful U.S. or coalition force. This protection may come from use of urban and other complex terrain and exploiting U.S. or coalition concerns about the attendant risk of civilian casualties or unacceptable collateral damage when engaging the enemy. Dispersion and the use of IW can also help protect the enemy. The enemy will try to conceal and protect the locations where its personnel plan IED operations, collect the necessary materials, make bombs, or train operatives for IED emplacement.

2-36. Operational shielding generally cannot protect the entire enemy organization for an extended time period. Rather, the enemy organization will seek to protect selected elements of its forces for enough time to gain the freedom of action necessary to execute IED operations.

NEUTRALIZE TECHNOLOGICAL OVERMATCH

2-37. Although the United States currently enjoys overwhelming military superiority, this no longer serves as an adequate deterrent against many emerging threats, especially those from nonstate actors. When conflict occurs, any enemy will seek ways to neutralize our technological advantage. Against a technologically superior force, enemy organizations will disperse their forces in areas where complex terrain limits the U.S. ability to apply our full range of technological capabilities. However, the enemy can rapidly mass forces from these dispersed locations to conduct IED operations at the time and place of its

own choosing. Enemy organizations train its forces to operate in adverse weather, limited visibility, rugged terrain, and urban environments. Such conditions can shield the enemy from the effects of U.S. or coalition force high-technology weapons and deny U.S. or coalition forces the full benefits of their advanced reconnaissance, intelligence, surveillance, and target acquisition (RISTA) systems.

High-Technology Targeting of United States Systems

2-38. Enemy forces might concentrate the use of IEDs on the destruction of high-visibility (flagship) U.S. systems. Losses among these premier systems may not only degrade operational capability, but also undermine U.S. or coalition morale. Thus, attacks against such targets are not always linked to military-style objectives.

Technology for Situational Understanding

2-39. The enemy will use its own RISTA means to support IED employment. The proliferation of advanced technologies permits some enemy organizations to achieve a SU of U.S. or coalition deployments and force dispositions formerly reserved for the militaries of technologically advanced nations. Much information on the sources of such technology is readily and cheaply available on the Internet and in open-source documents. These media can provide enemy forces with extensive information on U.S. or coalition members and their armed forces. Intelligence can also be obtained through greater use of human intelligence (HUMINT) assets that, among other sources, gain intelligence through sympathetic elements in the local population and from civilians or local workers contracted by U.S. or coalition forces for base operation purposes. Similarly, communication technologies are becoming more reliable and inexpensive. Therefore, they could act as a primary communication system or a redundant measure. There will be little U.S. or coalition forces can do to prevent the use of these assets, especially since it is becoming harder to discriminate between civilian and military-type usage.

Availability of Technology

2-40. Enemy forces use all the technology available to them, sometimes in adaptive or innovative ways. Low-technology solutions could be used against high-technology systems of an enemy. The construction of IEDs often involves employment of components for other than their originally intended purpose. Enemy forces take advantage of opportunities to upgrade available materials primarily through captured equipment, the black market, or outside support. See Chapter 4 for additional information.

Nonlinear Operations

2-41. IEDs are often employed in nonlinear operations. The enemy considers the difference between linear and nonlinear operations less in terms of geography and more in the terms of effects desired. Linear operations normally produce small effects from small actions and large effects from large actions (or perhaps large effects from an aggregation of small actions) in a linear relationship. Linear operations are proportional and additive, and typically produce a predictable, measurable effect. In contrast, this relationship may not always be present in nonlinear operations, which can produce large effects from small actions. In some cases, small actions produce small effects or no effects at all (for example, if an IED explodes without affecting the intended target). Thus, nonlinear operations can produce disproportionate, often unpredictable, effects.

Systems Warfare

2-42. The enemy can use IEDs in conducting systems warfare against U.S. or coalition systems. Because the focus of systems warfare is not just on the immediate target, but on the effects that can be created by striking that target, this approach could also fall under the label of "effects-based operations." In this approach, the enemy views its adversary as a collection of complex, dynamic, and interrelated systems and advocates the use of all elements of available power to create actions leading to desired effects on those systems. The intent is to identify critical system components and attack them in a way that will degrade or destroy the use or importance of the overall system.

2-43. Several things have to happen to wage systems warfare. Acknowledging the difficulty of successfully predicting outcomes in nonlinear, complex environments and the multitude of constantly occurring complex interactions, the enemy will develop possibilities or hypotheses about the systems of its opponent comprising the U.S. and its coalition coherence, will, and decision making.

2-44. Systems warfare requires detailed information on targets and their possible effects. The enemy will attempt to find and attack critical links, nodes, seams, and vulnerabilities in U.S. systems that offer the best opportunity to "level the playing field." This entails RISTA capabilities linked directly to IED operations that are tailored to affect specific capabilities whose loss or degradation will significantly reduce overall force effectiveness of U.S. or coalition forces.

2-45. Therefore, the enemy often targets the "soft" components of U.S. or coalition combat systems. Attacking U.S. or coalition logistics, command and control (C2), and RISTA can undermine the overall effectiveness of our combat system without having to directly engage our superior combat and combat support (CS) forces. IEDs can be the weapons of choice for doing so.

Note. A combat system is the "system of systems" that results from the synergistic combination of five basic subsystems that are interrelated to achieve a military function: combat forces, CS forces, logistics forces, C2, and RISTA.

2-46. IEDs are useful for systems warfare, as a means of attacking U.S. and coalition lines of communications (LOCs), convoys, and other logistics assets. They also provide a means to attack U.S. or coalition C2, combat forces, and CS forces without having to mount force-on-force attacks. In the nonlinear, distributed battlespace of a complex OE, some of the smallest activities and interactions can cause the greatest effects. No activity is subject to successful prediction.

CONTROL THE TEMPO

2-47. The enemy forces will try to execute IED operations at the time and place of their own choosing. IED activities may not be linked to other enemy actions or objectives. Rather, their purpose is to inflict mass casualties or destroy flagship systems (both of which reduce U.S. or coalition forces) and continue the fight.

2-48. Enemy forces can vary the tempo of IED operations. A period of relatively low activity in IED employment might lull U.S. or coalition forces into a false sense of security, making them more vulnerable to the next round of IEDs.

CHANGE THE NATURE OF THE CONFLICT

2-49. Enemy forces will try to change the nature of the conflict in order to exploit the differences between friendly and enemy capabilities and sensitivities and to present U.S. or coalition forces with conditions for which it is not prepared. Enemy organizations will adjust their IED TTP to the strengths and weaknesses of U.S. or coalition forces. The enemy is prepared to disperse his forces in areas of sanctuary and employ them in ways that present a battlefield that is difficult for U.S. or coalition forces to analyze and predict. Enemy forces may use a sympathetic population to provide refuge or a base of operations. They move out of sanctuaries and employ IEDs when they can create a window of opportunity or when physical or natural conditions present an opportunity. Also, they may use IEDs against U.S., coalition, or host nation (HN) civilians or Soldiers and Marines not directly connected to the intervention, as a device to change the fundamental nature of the conflict.

ALLOW NO SANCTUARY

2-50. Enemy forces seek to use IEDs to deny U.S. or coalition forces safe haven during every phase of a deployment and as long as they are in the region or threatening to intervene there. The resultant drain on U.S. or coalition manpower and resources to provide adequate force protection (FP) measures can reduce

strategic, operational, and tactical means to conduct war. Such actions will not only deny U.S. or coalition forces sanctuary, but also erodes their national will.

2-51. IEDs can be used to cause politically unacceptable casualties anywhere and at any time. However, they can be used at a particular time and/or place in order to deny U.S. or coalition forces access to an area, deny them safe haven, disrupt logistics, or impede movement. They can also be used to assassinate key military, government, or civilian figures or to target a particular group or organization. Physical casualties caused by IEDs also create a psychological effect that can intimidate or coerce others.

2-52. IED operations are basically nonlinear. The enemy, whether a nation-state or nonstate actor, will try to present U.S. or coalition forces with a nonlinear, simultaneous battlespace in which there is no safe "rear area." The enemy can use IEDs to attack our headquarters (HQ), logistics centers, and supply and evacuation routes. It can also use IEDs to attack our living quarters, dining facilities, and places frequented by our off-duty Soldiers, Marines, and civilians.

VARIED ACTIONS

2-53. Most of the above principles to some degree involve decentralized, dispersed, and distributed activities. To best attack superior forces, enemy leaders use initiative to conduct IED operations at a time and place of their choosing. This may mean acting at a time and place and under circumstances to offset U.S. advantages and maximize sanctuary from effects of U.S. or coalition systems. The enemy also varies the types of IEDs it employs and the methods of employment. This can make pattern analysis and templating challenging for U.S. or coalition forces.

This page is intentionally left blank.

Chapter 3

Improvised Explosive Device Threat

Although virtually any person or type of conventional or paramilitary group may employ an IED, it is a proven and effective weapon for insurgents, terrorists, and other nonstate actors. Such groups may or may not be linked to a political state and are not limited by geographic boundaries. Their motivations are often ideological and do not share the same characteristics or centers of gravity as those found in a typical state versus state conflict. They are typically organized in a nonhierarchical, nonlinear network of cells. The structure resembles that of a communication network, such as the Internet, and its nonlinearity makes it extremely survivable. There are often many communication paths and decentralized C2. Some of these networks are independent and range from the theater down to the village level. Others are linked together to provide coordinated attacks against U.S. and coalition forces and are a part of large international terrorist organizations. The rapid technological advances in communication devices (such as wireless) and the Internet provide low-cost and easily obtainable modes of communication.

3-1. Regardless of the type of group that systematically employs IEDs, key functions must be performed. These functions can be described as a nonlinear system, and critical personnel, actions, and resources determine the enemy IED system. The enemy IED activity model in Figure 3-1, page 3-3, describes the key nodes in a system designed to conduct IED attacks. Many of these nodes are part of the operation of a larger nonstate group. Successful IED defeat requires the commander to influence a subset of these functions to defeat the IED threat. The interconnections depicted in Figure 3-1 represent the impact one node may have on another. For example, local support will make it easier for the enemy to recruit and find supplies. These interconnections will be used to determine the level of effect that attacking a node has on the overall capability of the enemy. Descriptions of enemy nodes include—

- **International leadership.** International leadership is a person or group that provides the overall direction and purpose for the group if it is transnational in nature. This leadership may coordinate the relationship between the nodes and conduct strategic planning.
- **Regional and local leadership.** These nodes describe the leadership required to carry out the operations delegated by the overall group leadership. A network can also be made up of many splinter organizations carrying out specific orders from a larger, more centralized coordination group.
- **Recruitment.** Recruitment is the activities related to the act of building a force of operatives, trainers, financers, and technicians to carry out the campaign of the group.
- **Training.** Training is the act of providing a means to educate recruited personnel in a skill needed to perform a role in the overall effort. Some personnel may be trained as engineers, while others may be trained to emplace IEDs.
- **Target selection and planning.** Planners must first select a target before mission planning can begin. Through observation, the enemy collects valuable information on troop movement, times of vulnerability, target vulnerability, and areas of approach and escape. IED operations will become more complex as friendly security and IED defeat capabilities grow.
- **Surveillance.** Surveillance is to observe potential targets in order to collect information used in the planning of IED operations. These observations aid the enemy planner with critical information, such as ideal IED emplacement locations, high-traffic areas, concealment data, observation points, and avenues of escape and reinforcement.

- **Attack rehearsal.** A rehearsal both prepares the IED team for its actions and tests and evaluates the plan of attack.
- **Regional and local support.** Active local support consists of citizens and other locals assisting with enemy IED efforts (such as looking out for troops while IEDs are being placed or donating supplies). Passive local support for insurgent IED efforts consists of the refusal of citizens and other locals to give U.S. or coalition forces information or assistance. Passive local support of IED efforts result in part from fear of reprisal, but may also be attributed to sympathy with enemy objectives.
- **Movement.** Movement is the physical movement of devices, supplies, and personnel into and out of an AO during predetonation and postdetonation phases.
- **Funding.** Funding is the means and methods used to subsidize the cost of IED operations.
- **Supplies.** Supplies are the materials and the availability of materials used to accomplish IED operations.
- **Improvised explosive device makers.** IED makers are the persons involved in the design and fabrication of an IED.
- **Orders group.** The orders group (which may have no formal name) is a small cell made up of one or more members of the regional and/or local leadership and possibly the IED makers. It is designed to coordinate the IED effort while compartmenting information in case of infiltration or discovery.
- **Improvised explosive device team.** The IED team is the personnel who emplace, monitor, and detonate the IED.
- **International support.** International support is support in the form of funding, training, organization, recruiting, publicity, and planning assistance that is provided to the group from nonlocal sources, to include foreign nations and states, NGOs, terrorist organizations, media outlets, and other organizations or individuals.
- **Emplacement.** Emplacement is the positioning of an IED for the purpose of conducting an attack.
- **Improvised explosive device monitoring and detonating.** To monitor and detonate IEDs is the act of observing the area of emplacement in order to command detonate an IED.
- **Battle damage assessment.** Battle damage assessment (BDA) is the act of observing the detonation or aftermath of an explosion to evaluate the destruction of the IED. Often this is a decision point for the enemy to initiate a follow-on attack or egress out of the kill zone.
- **Infrastructure.** IED makers require an infrastructure of safe houses, work areas, and storage facilities.
- **Information campaign.** The enemy can be very effective using IW as a method of promoting group success, which fuels recruiting efforts and encourages support by portraying a positive image of the operations of the group.

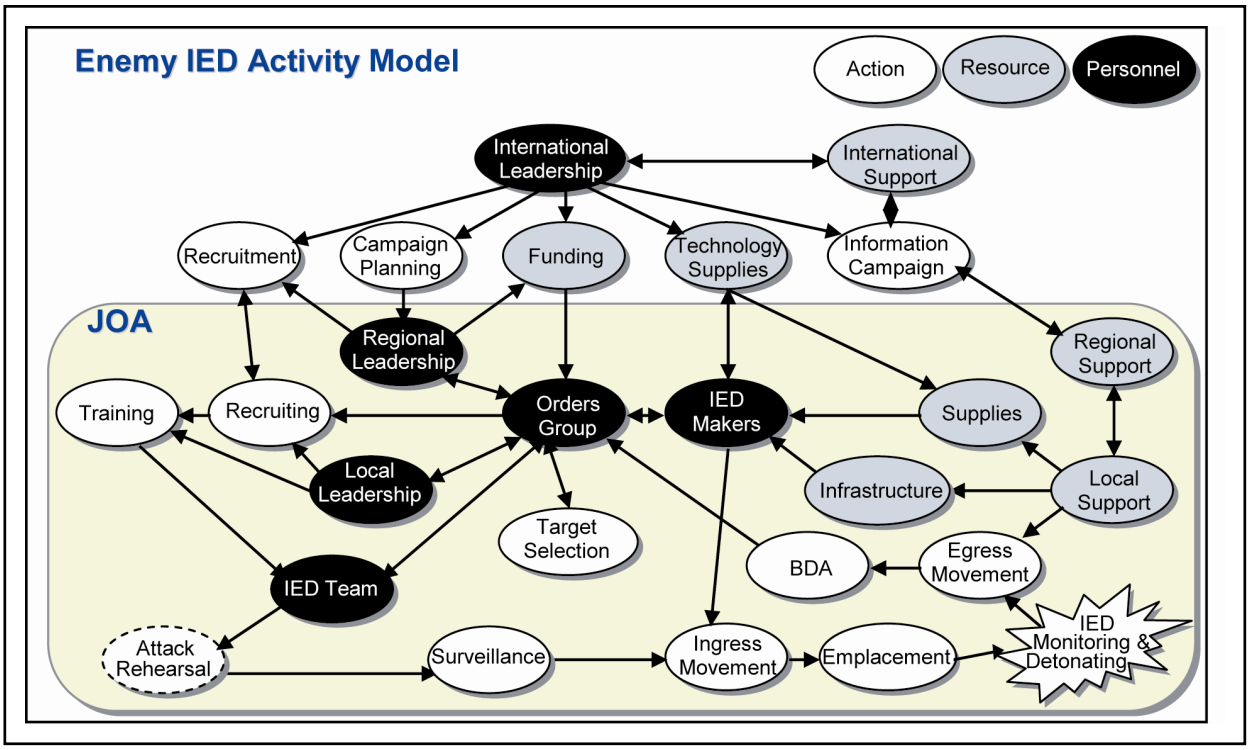

Figure 3-1. Enemy IED system

3-2. Figure 3-1 shows that there are multiple vulnerabilities that the joint task force (JTF) commander can exploit to bring about IED defeat. It is not necessary to attempt to prevent the detonation of every IED. By attacking or isolating one or more key actions (resources or groups of personnel), the JTF commander can prevent the effects of IEDs in a proactive manner.

3-3. The challenge is to identify which nodes the JTF commander can affect and which of those has the largest payoff for IED defeat. Enemy activity nodes fall into different levels of influence from the national to the tactical level. Successful attacks against the enemy will require a joint interagency effort including the DOD, the intelligence community, law enforcement, and interaction with international partners.

This page is intentionally left blank.

Chapter 4

Improvised Explosive Device Characteristics

WARNING

Specific identification features for IEDs are ever-changing based on the capabilities and available resources of the enemy.

DANGER

Do not attempt to move, approach, or take any action on a possible IED. If possible, avoid using any communication or electronic equipment within the established exclusion area. Any of the above dangers may cause an IED to detonate.

IEDs are a dangerous and effective weapon system that military forces face. IEDs can be almost anything with any type of material and initiator. They are an improvised device that are designed to cause death or injury by using explosives alone or in combination with other materials, to include projectiles, toxic chemicals, biological toxins, or radiological material. IEDs can be produced in varying sizes and can have different types of containers and functioning and delivery methods. IEDs can use commercial or military explosives, homemade explosives, or military ordnance and ordnance components. IEDs are primarily conventional high-explosive charges, also known as homemade bombs. A chemical and biological (CB) agent, or even radiological material, may be included to add to the destructive power and the psychological effect of the device. They are unique in nature because the IED builder has had to improvise with the materials at hand. Designed to defeat a specific target or type of target, they generally become more difficult to detect and protect against as they become more sophisticated. IEDs are becoming increasingly sophisticated and can be fabricated from common materials. IEDs may range in size from a cigarette pack to a large vehicle. The degree of sophistication depends on the ingenuity of the designer and the tools and materials available. IEDs of today are extremely diverse and may contain any type of firing device or initiator, plus various commercial, military, or contrived chemical or explosive fillers. Cached, stockpiled munitions, or CEA within the current theater of operations may provide the explosive materials to "would be" enemy bombers.

COMPONENTS

4-1. IEDs can vary widely in shape and form (Figure 4-1, page 4-2) IEDs share a common set of components and consist of the main charge, initiating system, and casing.

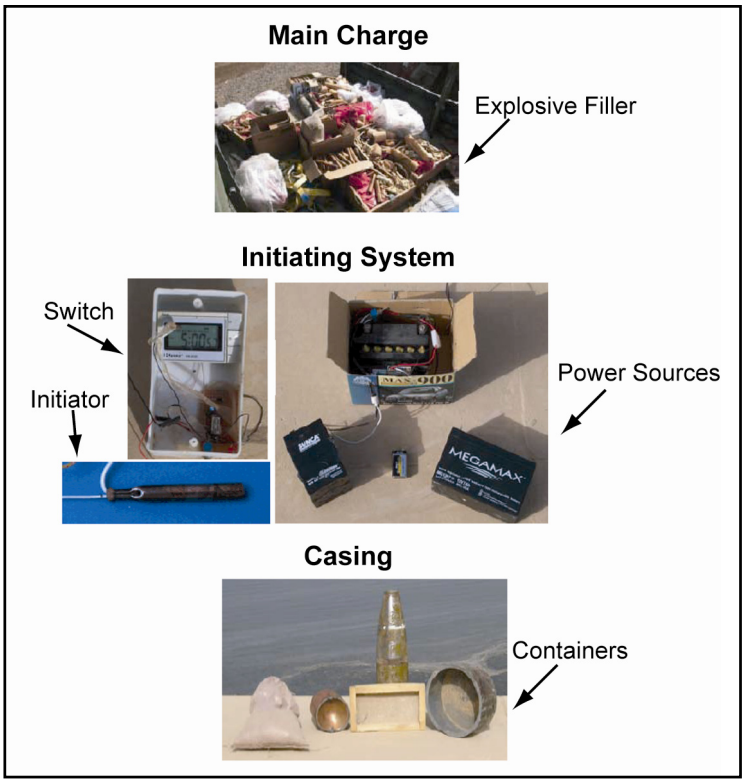

Figure 4-1. Components of an IED

MAIN CHARGE

4-2. The most common explosives used are military munitions, usually 122-millimeter or greater mortar, tank, and/or artillery rounds. These items are the easiest to use and provide a ready-made fragmentation effect and they allow for relatively easy "daisy chaining," which is linking multiple main charges together over long or short distances for simultaneous detonation. Other IEDs have used military and commercial explosives, such as PE4, trinitrotoluene (TNT), ammonium nitrate (fertilizer), and fuel oil (ANFO). Common hardware, such as ball bearings, bolts, nuts, or nails, can be used to enhance the fragmentation. Propane tanks, fuel cans, and battery acid can and have been added to IEDs to propagate the blast and thermal effects of the IED.

INITIATING SYSTEM

4-3. The initiation system or fuze functions the device. It could be a simple hard wire for command detonation to a cellular telephone or remote controls to toy cars and airplanes for radio-controlled IEDs. The initiator almost always consists of a blasting cap.

4-4. Batteries are used as a power source for detonators. Batteries of all types are the primary source of power for IEDs. Batteries could be as small as 9-volts, AA, and those used in long-range cordless telephones (LRCTs) to car and truck batteries. IEDs may even be wired into the local power supply of a home or office.

CASING

4-5. Casings can range in size from a cigarette pack to a large truck or airplane. The container is used to help hide the IED and to possibly provide fragmentation. A myriad of containers have been used as casings, including soda cans, animal carcasses, plastic bags, and vests or satchels for suicide bombers.

INITIATION METHODS

4-6. Initiation methods (Figure 4-2) include—

- **Time.** Time IEDs are designed to function after a preset delay, allowing the enemy to make his escape or to target military forces which have created a pattern. Timers used include igniferous, chemical, mechanical, and electronic.
- **Command.** Command-initiated IEDs are a common method of employment and allow the enemy to choose the optimum moment of initiation. They are normally used against targets that are in transit or where a routine pattern has been established. The most common types of command-initiated methods are with command wires or radio-controlled devices, such as LRCTs, cordless telephones, and remote car openers and alarms.
- **Victim.** A victim-actuated IED is a means of attacking an individual or group of individuals. There are various types of initiation devices, which include pull or trip, pressure, pressure release, movement-sensitive, light-sensitive, proximity, and electronic switches.

WARNING

Specific identification features for IEDs are ever-changing based on the capabilities and available resources of the enemy.

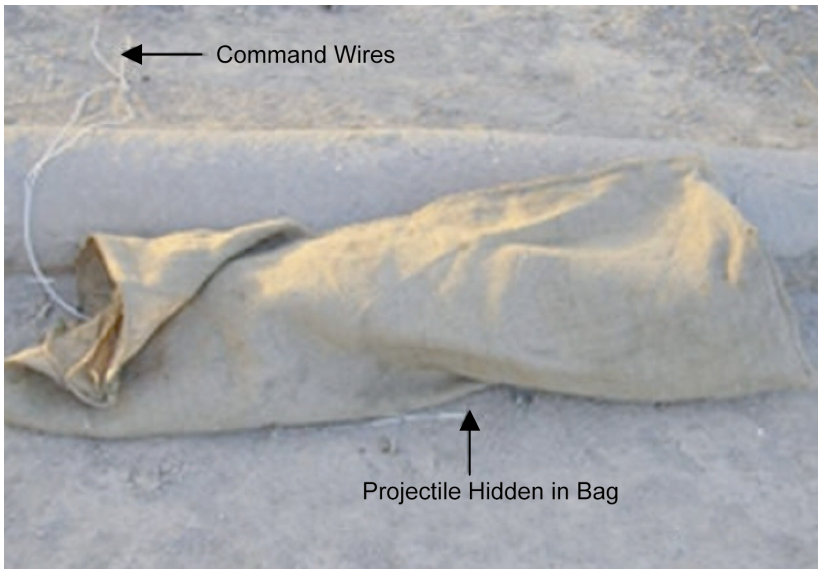

Figure 4-2. Command-initiated concealed IED

USES AND TARGETS

4-7. IEDs can be used in the following manners:

- Disguised static IEDs can be concealed with just about anything (trash, boxes, tires, and so forth) and can be placed in, on, or under a target or in or under unsecured vehicles.
- Disguised moveable IEDs (vehicle-borne improvised explosive devices [VBIEDs], suicide bomber vests, victim-actuated IEDs, or remote-controlled cars).
- Thrown or projected IEDs (improvised grenades or mortars), used mostly from overhead passes.
- IEDs placed in, on, or under a target or in or under unsecured vehicles.

- Hoax IEDs which the enemy uses for a myriad of purposes, such as to learn our TTP, entrapment, nonexplosive obstacle, and development of complacency for future IED attacks. Hoax IEDs include something resembling an actual IED, but have no charge or a fully functioning initiator device.

4-8. IEDs can be designed to attack specific targets, such as high-visibility targets, high-value targets (dignitaries), and military targets, such as—

- Quick-reaction forces (QRFs) and first responders.
- Cordons.
- Checkpoints and control points.
- Logistics movements or combat patrols.
- Anywhere that a targetable pattern has developed.

Note. Secondary and tertiary IEDs should be expected in the area.

INDICATORS

4-9. The primary indication of an IED will be a change in the environment (something new on the route that was not there yesterday). The enemy may leave behind visual indicators of an emplaced IED by accident or on purpose (to inform the local population). Vigilant observation for these subtle indicators can increase the likelihood of IED detection by friendly forces before detonation. Examples of possible roadside IED indicators include, but are not limited to—

- Unusual behavior patterns or changes in community patterns, such as noticeably fewer people or vehicles in a normally busy area, open windows, or the absence of women or children.
- Vehicles following a convoy for a long distance and then pulling to the roadside.
- Personnel on overpasses.
- Signals from vehicles or bystanders (flashing headlights).
- People videotaping ordinary activities or military actions. Enemies using IEDs often tape their activities for use as recruitment or training tools.
- Suspicious objects.
- Metallic objects, such as soda cans and cylinders.
- Colors that seem out of place, such as freshly disturbed dirt, concrete that does not match the surrounding areas, colored detonating cord, or other exposed parts of an IED.
- Markers by the side of the road, such as tires, rock piles, ribbon, or tape that may identify an IED location to the local population or serve as an aiming reference (such as light poles, fronts or ends of guardrails, and road intersections or turns).
- New or out of place objects in an environment, such as dirt piles, construction, dead animals, or trash.
- Graffiti symbols or writing on buildings.
- Signs that are newly erected or seem out of place.

4-10. Friendly forces should be especially vigilant around—

- Obstacles in the roadway to channel convoys.
- Exposed antennas, detonating cord, wires, or ordnance.
- Wires laid out in plain site; these may be part of an IED or designed to draw friendly force attention before detonation of the real IED.

LOCATIONS

4-11. IEDs may be emplaced anywhere that enough space exists or can be created to hide or disguise the IED. Whenever possible, devices are located where employment can exploit known U.S. patterns (such as

the use of a main supply route [MSR]) or vulnerabilities (such as soft-skinned vehicles or chokepoints). Common areas of IED emplacement (Figure 4-3) include, but are not limited to—

- Previous IED sites (past successes).
- Frequently traveled, predictable routes, such as roads leading to FOBs and along common patrol routes.
- Boundary turn around points (pattern).
- Roadway shoulders (usually within 10 feet).
- Medians, by the roadside, or buried under the surface of any type of road, often in potholes and covered with dirt or reheated asphalt.
- Trees, light posts, signs, overpasses, and bridge spans that are elevated.
- Unattended vehicles, trucks, cars, carts, or motorcycles (attached or installed in them).
- Guardrails (hidden inside) or under any type of material or packaging.
- Potential incident control points (ICPs).
- Abandoned structures (sometimes partially demolished).
- Cinder blocks (hidden behind) or piles of sand to direct blast into the kill zone.
- Animal carcasses and deceased human bodies.
- Fake bodies or scarecrows in coalition uniforms.
- Buildings.

Note. See Appendix B, paragraph B-5, for particularly suitable IED locations.

Figure 4-3. Common areas of IED emplacement

This page is intentionally left blank.

Chapter 5

Organizations Involved in Improvised Explosive Device Defeat

See Appendix C for contact information on these organizations. This is not an all inclusive list of organizations involved in IED defeat. All organizations listed in Appendix C have Internet links to other organizations.

ASYMMETRIC WARFARE GROUP

5-1. The Asymmetric Warfare Group (AWG) conducts operations in support of joint and Army force commanders to mitigate and defeat specified asymmetric threats. The AWG—

- Provides, deploys, integrates, coordinates, and executes C2 of trained and ready forces.
- Seeks, collects, develops, validates, and disseminates emerging TTP.
- Assists in exploitation and analysis of asymmetric threats.
- Provides advisory training for in-theater or predeployment forces.
- Provides identification, development, and integration of countermeasure technologies.

CAPTURED MATERIEL EXPLOITATION CENTER

5-2. The Captured Materiel Exploitation Center (CMEC) is formed from the assets of organic and attached technical intelligence (TECHINT) elements augmented by other subject matter experts (SMEs). It manages the command battlefield TECHINT system through the military intelligence (MI) brigade and the Assistant Chief of Staff, Intelligence (G-2). When possible, other armed services should combine assets for the acquisition and exploitation of captured enemy munitions, to include CEA. When this occurs, the CMEC becomes the Joint Captured Material Exploitation Center (JCMEC).

CHEMICAL, BIOLOIGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH-YIELD EXPLOSIVE COMMAND

5-3. The Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Command is assigned to the United States Army Forces Command (FORSCOM) and brings C2 of the Army's most specialized weapons of mass destruction (WMD) operational assets together. This provides a single point of contact within the Army for the DOD to call when a coordinated response to the threat or use of WMD is needed anywhere in the world. CBRNE Command maintains C2 of Army EOD forces.

5-4. The mission of the CBRNE command is to C2 organic and allocated Army technical assets to support full-spectrum CBRNE technical operations that detect, identify, assess, render-safe, dismantle, transfer, and dispose of CBRNE incident devices and materiel including UXO and IEDs. The command is also responsible for managing DOD technical support to consequence management operations and providing CBRNE technical advice and subject matter expertise.

5-5. This deployable operational-level command manages existing and future programmed CBRNE response assets that can simultaneously respond to multiple CBRNE incidents in support of combatant commanders and the joint team at home and around the world. Its subordinate units include two explosive ordnance groups, five ordnance battalions, two technical escort chemical battalions, and operational control of the Army Reserve Unit—Consequence Management. Future growth of the command includes the

activation of two subordinate ordnance battalions, a chemical brigade HQ, and an analytical and remediation directorate.

COMBINED EXPLOSIVES EXPLOITATION CELL

5-6. The Combined Explosives Exploitation Cell (CEXC) is a joint agency team tasked with the collection and exploitation of IEDs. CEXC provides immediate in-theater technical and operational analysis of IEDs and develops measures to counter bombing campaigns; collects and exploits TECHINT and forensic evidence from explosives related incidents (with major emphasis on IED components); and collect construction and techniques in order to determine enemy tactics, identify trends, target IED bomb makers; and enable both offensive and defensive counter-IED operations by coalition forces. Critical tasks include—

- Conducting first-line technical exploitation and evaluation of IEDs and components and preparing detailed laboratory reports for all exploited material.
- Providing advice on EOD, FP, and combat tactics in regard to the threat posed by IEDs.
- Attending all significant IED/explosives related incidents.
- Exploiting cache discoveries containing large quantities of military ordnance, bomb-making materials, and/or homemade explosive manufacturing and storage sites.
- Exploiting any incident site where the collection of forensic evidence is important.
- Providing detailed field forensics analysis for targeting.
- Preparing, publishing, and disseminating throughout theater, a comprehensive report for every incident attended and a weekly report summarizing IED incident statistics, significant events, and recovered devices for the last seven days.
- Preparing, publishing, and disseminating throughout theater, spot reports and technical bulletins for rapidly emerging threats, significant incidents, and newly seen devices.
- Providing technical assistance to support the interrogation of IED-related detainees.
- Providing technical advice on FP issues and counter-IED TTP.
- Providing assistance for operations against suspected bomb makers and transporters, IED factories, storage locations, and training sites.
- Providing briefings, component familiarization, personnel, and SME support.

COUNTER EXPLOSIVE HAZARDS CENTER

5-7. The Counter Explosive Hazards Center (CEHC) develops, synchronizes, trains, and integrates counter explosive hazard (mines, UXO, IEDs, booby traps) solutions across the DOTMLPF spectrum. CEHC supports the fundamentals of assured mobility, protect the force in the contemporary and future OEs, and maintain expertise in counter explosive hazard warfare.

ENGINEER UNITS

5-8. The specific combat engineer missions concerning explosive hazard are breaching, clearing, and proofing minefields. In extreme high-operational tempo or high-intensity combat missions, U.S. Army engineers or other non-EOD units may conduct limited reduction or clearing of non-mine explosive hazard and IED hazards, under the technical guidance of Army EOD forces. During the post-conflict phase, engineers may also assist EOD forces in battlefield UXO cleanup operations, as required. JP 3-34, JP 4-04, FM 3-34, and FM 5-116, provide more details on specific engineer units and tasks.

CLEARANCE COMPANY

5-9. A clearance company (Army only) conducts detection and limited IED neutralization (as outlined in Chapter 6) along routes and within areas of support to enable force application, focused logistics, and protection. It provides training readiness and oversight of assigned route and area clearance platoons. The company provides battle command for 3- to 5-route, area, or Sapper platoons. It is capable of clearing a

total of 255 kilometers of two-way routes per day (three routes of 85 kilometers each) and can clear a total of two acres per day (two areas at one acre each).

Route Clearance Platoon

5-10. The mission of a route clearance platoon is to conduct route reconnaissance, minesweeping, enemy or unobserved minefield clearance operations, and deliberate route clearance. It clears obstacles with engineer (countermine) equipment or uses demolitions and performs engineer reconnaissance. The platoon provides digital hazard area data to other units at the objective and is fully mobile in-theater using organic assets only. It is capable of—

- Clearing and marking 85 kilometers (daylight only) of route (4 meters wide) per day (enemy capability and terrain dependent).
- Identifying and neutralizing mines, IEDs (as outlined in Chapter 6), and UXO on routes.
- Receiving and analyzing Ground Standoff Mine Detection System (GSTAMIDS) and Airborne Standoff Minefield Detection System (ASTAMIDS) data from other units.

Area Clearance Platoon

5-11. The mission of an area clearance platoon is to conduct area clearance, minesweeping, and enemy or unobserved minefield clearance operations. The platoon clears obstacles with engineer (countermine) equipment or uses demolitions and performs engineer reconnaissance. It is fully mobile in-theater using organic assets only. It is capable of—

- Clearing and proofing 0.004 square kilometers per day of mines (buried and surface), IEDs (as outlined in Chapter 6), and UXO (daylight only).
- Extracting casualties from an explosive hazard area.
- Providing digital hazard area information to other units (objective).

ENGINEER MINE DOG DETACHMENT

5-12. The Engineer Mine Dog Detachment consists of trained mine detection dog teams with specialized search dog capability. Engineer mine detection dogs are trained for the military OE to perform area and route clearance and search, minefield extraction, combat patrols, building search (disruptive and nondisruptive), vehicle search, and cave clearance. The dogs can reduce the time spent on a search. Dogs can search in open areas, fields, woods, hedgerows, and embankments. They are an excellent tool to route proof along roads, tracks, and railways. They can detect metallic and nonmetallic mines, both buried and surface laid. Dogs increase the speed and efficiency of an IED defeat operation.

EXPLOSIVE HAZARDS COORDINATION CELL

5-13. The mission of the explosive hazards coordination cell (EHCC) is to enable the land component commander to predict, track, distribute information on, and mitigate explosive hazards within the theater that affect force application, focused logistics, protection, and battlespace awareness. The EHCC establishes and maintains an explosive hazard database, conducts pattern analysis, and investigates mine and IED strikes and UXO hazard areas. The cell provides technical advice on the mitigation of explosive hazards, including the development of TTP, and provides training updates to field units. They coordinate explosive hazard teams (EHTs). The EHCC capabilities include—

- Establishing, maintaining, and sharing the explosive hazard tracking database within the joint operations area (JOA).
- Ensuring accuracy of explosive hazard information distribution via the battle command system.
- Coordinating site evaluations and/or strike incident investigations at four sites simultaneously or conducting unit training at four sites simultaneously.
- Assisting ISR planners with explosive hazard pattern analysis and intelligence collection management.

- Coordinating technical and tactical training for the brigade combat teams (BCTs) by the EHTs.
- Providing updated TTP and guidance for route and area clearance operations.

5-14. The EOD group or battalion and the EHCC coordinate and synchronize explosive hazard information and capability throughout the COP and JOA.

Explosive Hazards Team

5-15. The mission of an EHT is to provide evaluation of explosive hazard incident sites in support of BCTs and joint, interagency, and multinational (JIM) brigade-sized units and smaller. The EHT capabilities include—

- Conducting site evaluation of explosive hazard incident sites (to include CEA, multiple UXO, and post-blast analysis).
- Conducting TTP training (explosive hazards awareness training [EHAT], PSS-14, and area clearance) for BCT and JIM personnel on explosive hazard mitigation in a JOA.
- Conducting annual recertification, quarterly reinforcement, and predeployment training of explosive ordnance clearance agent (EOCA) personnel. (This is an Army capability only.)
- Providing advice on explosive hazards as requested.
- Providing information into the explosive hazard database via the battle command system.
- Conducting disposal of limited explosive hazards; however, EHTs are not equipped to conduct RSPs on explosive hazards.
- Consolidating and conducting analysis of requests for modifications to the JOA UXO supplemental list.
- Providing recommendations to the CBRNE cell for modification of the JOA UXO supplemental list.

5-16. The EOD company and EHT coordinate and synchronize explosive hazard information and capability throughout the COP and area of responsibility (AOR).

Explosive Ordnance Clearance Agent

5-17. EOCA personnel (Army only) are combat engineers trained to perform limited battlefield disposal of UXO as outlined in the EOCA identification guide and the JOA UXO supplemental list. If the UXO is out of the scope of operations for the EOCA, EOD personnel must be called. EOCA personnel can assist EOD personnel in disposing of other explosive hazards as requested. Properly trained and certified EOCA capabilities include—

- **Unexploded ordnance reconnaissance.** EOCA personnel are trained to perform detailed reconnaissance of a suspected UXO.
- **Unexploded ordnance identification.** EOCA personnel can perform limited identification of the items listed in the EOCA identification guide and the JOA UXO supplemental list. Items that the EOCA cannot positively identify must be reported to EOD personnel.
- **Unexploded ordnance area marking.** EOCA personnel mark the UXO area according to the standard UXO marking system.
- **Protective works.** EOCA personnel can provide the blast and fragmentation danger area of identified UXO. EOCAs may provide the estimated blast and fragmentation danger area for items similar to but not included in the EOCA identification guide and the JOA UXO supplemental list. EOCAs will advise the on-scene commander with the recommended personnel and equipment protective measures. When the commander determines that certain personnel or equipment cannot be removed from the hazard area, protective works must be established to protect those personnel and assets from the effects of the UXO. EOCAs will recommend and supervise the appropriate protective works to be completed.
- **Unexploded ordnance disposal.** EOCA personnel are authorized to destroy (by detonation) individual UXO identified in the EOCA identification guide and the JOA UXO supplemental list.

5-18. The following are the EOCA's limitations:

- Cannot move, combine, and/or destroy multiple UXO (such as a cache).
- Cannot do reconnaissance or do handling of IED or VBIED incidents.
- Can only perform CEA operations under the direct supervision of EOD personnel (includes EHTs).
- Are not to be used for explosive hazard response calls. However, if EOD is not readily available as determined by the maneuver commander, EOCA personnel can be used to conduct an initial reconnaissance of the UXO. If the UXO falls within their capability, then EOCA personnel may dispose of the UXO.

Note. The CBRNE cell at the Army theater land force or joint support manages modifications to the JOA UXO supplemental list. Requests to modify the supplemental list will be coordinated through the local EOD unit or EHT for approval by the CBRNE cell.

MINE AND EXPLOSIVE ORDNANCE INFORMATION AND COORDINATION CENTER

5-19. The Mine and Explosive Ordnance Information and Coordination Center (MEOICC) assists in the development of the COP and provides informational and SU on explosive hazards to all coalition forces, the National Mine Action Authority (NMAA), and NGOs to minimize casualties and equipment damage to coalition forces and the civilian populace and to support stability and reconstruction operations and humanitarian demining operations. The MEOICC conducts information management and exchanges information concerning explosive hazards with sector and division cells and the Coalition Provisional Authority (CPA); provides an interface with the CPA through the NMAA; provides explosive hazards awareness and mine detector training teams; and has oversight responsibility for geospatial and topographic products and weapons intelligence. MEOICC key tasks include—

- Training the forces in explosive hazards antitank (AT) mine detection.
- Maintaining the explosive hazards database (EHDB).
- Ensuring that equipment is funded and employed correctly.
- Tracking NGO operations within their AO.
- Transitioning operations to a designated military or civilian authority.

Note. The MEOICC will be replaced by the EHCC.

MOBILITY AUGMENTATION COMPANY

5-20. A mobility augmentation company (MAC) conducts assault gap crossings, mounted and dismounted breaches, and emplaces obstacles in support of maneuver BCTs and support brigades to enable force application, focused logistics, and protection.

SAPPER COMPANY

5-21. The mission of a Sapper company is to execute mobility, countermobility, and survivability tasks and to provide support of maneuver and support brigades to enable force application, focused logistics, and protection. A Sapper company reinforces engineers in maneuver BCTs.

TERRAIN TEAM

5-22. Terrain teams are deployed at the brigade, division, and corps levels to provide terrain analysis and geospatial support to the field. Counter-IED related support includes route analysis, identification of choke points, avenues of approach, line-of-sight analysis, and other tactical decision aids (TDAs). Terrain teams can also perform geospatial pattern analysis of tracking and locating IEDs. They provide the geospatial input to the IPB process.

EXPLOSIVE ORDNANCE DISPOSAL UNITS (ALL SERVICES)

5-23. EOD companies are on call 24 hours a day to provide emergency response teams in support of military missions, public safety, and law enforcement authorities at the federal, state, and municipal level. Each company can field 5 to 7 response teams depending on the manning configuration of the teams and the mission requirements. Each team is matched with a tailored equipment set and vehicle. Teams with equipment can be airlifted via rotary and fixed wing aircraft. EOD capabilities include—

- Identifying, rendering safe, and disposing of conventional/unconventional explosives and/or CBRNE munitions or devices (U.S. or foreign origin), to include IEDs. (EOD units are the only forces trained and equipped to render safe and dispose of IEDs.)
- Maintaining an EOD incident database located above division in the protect cell.
- Providing technical expertise to EHCCs and EHTs on explosive hazards.
- Acting as the SME for explosive hazards (IEDs, UXO, and CEA) to commanders (BCT, maneuver enhancement [ME] brigades, corps, divisions, and so forth).
- Conducting post blast and crater analysis.
- Conducting on-site assessment/verification for the presence of CBRNE material.
- Formulating a COA to protect forces, citizens, or operations from death, injury, or cessation of operations threatened by UXO, IED, or CBRNE.
- Performing chemical-biological testing in Occupational Safety and Health Administration (OSHA) Level A and Level B protective ensembles, military toxicological agent protective ensembles, or mission-oriented protective posture (MOPP)/joint services lightweight integrated-suit technology (JSLIST). Performing IED and UXO RSPs in ballistic protective "bomb suits" using an array of sets, kits, and outfits for disruption/defeat of devices and extensive technical manuals (CBRNE and conventional munitions/devices).
- Establishing working relationships with the Federal Bureau of Investigation (FBI) Bomb Data and Bureau of Alcohol, Tobacco, and Firearms (U.S.) (BATF) Arson and Explosives National Repository Centers; the Defense Intelligence Agency (DIA) Counterterrorism (CT) Division; the Missile and Space Intelligence Center, National Ground Intelligence Center (NGIC); National Laboratories; the Naval EOD Technical Center; and the Soldier and Biological Chemical Command (U.S. Army) (SBCCOMs) Technical Escort Unit.

UNITED STATES MARINE CORPS CHEMICAL BIOLOGICAL INCIDENT RESPONSE FORCE

5-24. The United States Marine Corps Chemical Biological Incident Response Force (CBIRF) provides a rapid response force for WMD incidents; consequence management support in military and industrial agent identification; downwind hazard prediction; advanced lifesaving support; casualty reconnaissance, extraction and triage; personnel decontamination; medical treatment; and stabilization for incident site management, including ordnance disposal, security, and patient evacuation. An EOD detachment in the CBIRF force protection element provides specialized response capabilities.

FOREIGN MATERIEL INTELLIGENCE GROUP

5-25. At echelons above corps (EAC), the Foreign Materiel Intelligence Group (FMIG) is a battalion-sized organization located at Aberdeen Proving Ground, Maryland. This group is the only active duty TECHINT unit in the Army. Responsibilities of the FMIG include—

- Conducting TECHINT operations.
- Preparing TECHINT reports in support of Army, joint, and combined operations.
- Acting as the Headquarters, Department of the Army (HQDA) executive agent for foreign materiel used for training purposes.

JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT TASK FORCE

5-26. The JIEDD TF focuses all counter-IED efforts within the DOD, while concurrently engaging other outside sources of potential solutions, to defeat current and future IED threats endangering joint and coalition forces. It is chartered to adopt a holistic approach focused on intelligence, TTP, information operations (IO), and the tenets of assured mobility (mitigation, prediction, detection, prevention, and neutralization). The goal is to identify and neutralize enemy leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs against coalition forces. At the same time, the TF is focused on training our own forces in the most current TTP being used by the enemy and the best available U.S. TTP to eliminate the IED threat.

5-27. The JIEDD TF has developed a full spectrum analysis of IEDs that considers and applies multiple DOTMLPF strategies to effectively counter the IED threat. This counter-IED effort is a combined joint service, interagency, multinational program designed to leverage all available resources and technologies in a coordinated campaign to defeat the IED threat. To facilitate this effort a Joint Senior Advisory Group (JSAG) (comprising representatives from all the services, the joint staff, the Office of the Secretary of Defense, and the United Kingdom) has been formed to evaluate issues for decision by the joint IED defeat integrated process team.

MILITARY INTELLIGENCE UNITS

5-28. MI units assist the commander in visualizing his battlespace, organizing his forces, and controlling operations to achieve the desired tactical objectives or end-state. Intelligence supports FP by alerting the commander to emerging threats and assisting in security operations. The commander must understand how current and potential enemies organize, equip, train, employ, and control their forces. Intelligence provides an understanding of the enemy, which assists in planning, preparing, and executing military operations. One of the most significant contributions that intelligence personnel can accomplish is to accurately predict future enemy events. Although this is an extremely difficult task, predictive intelligence enables the commander and staff to anticipate key enemy events or reactions and develop corresponding plans or counteraction. Commanders must receive the intelligence, understand it (because it is tailored to the commander's requirements), believe it, and act on it.

5-29. Intelligence tasks include—

- Supporting SU, to include—
  - Performing IPB.
  - Performing situational development.
  - Providing intelligence support to FP.
- Supporting strategic responsiveness, to include—
  - Performing indications and warning (I&W) to ensure intelligence readiness.
  - Conducting area studies of foreign countries.
  - Supporting sensitive site exploitation.
- Conducting ISR, to include—
  - Performing intelligence synchronization.
  - Performing ISR integration.
  - Conducting tactical reconnaissance.
  - Conducting surveillance.
  - Providing intelligence support to effects, to targeting, IO, and combat assessment.

NATIONAL GROUND INTELLIGENCE CENTER

5-30. The NGIC produces and disseminates all-source-integrated intelligence on foreign forces, systems, and supporting combat technologies to ensure that U.S. forces have a decisive edge on any battlefield. NGIC provides all-source analysis of the threat posed by IEDs produced and used by foreign terrorist and insurgent groups. NGIC supports U.S. forces during training, operational planning, deployment, and

redeployment. NGIC maintains a counter-improvised explosives device targeting program (CITP) portal on the Secure Internet Protocol Router Network (SIPRNET) Web site that provides information concerning IED activities and incidents, and NGIC IED assessments. In the IED fight, NGIC increases the capability of the coalition force to collect TECHINT and provide dedicated intelligence fusion in order to target bomb makers and their networks. NGIC provides weapons intelligence teams (WITs), which are deployed to brigade level to assist with IED incidents.

NAVAL EXPLOSIVE ORDNANCE DISPOSAL TECHNOLOGY DIVISION

5-31. The Naval Explosive Ordnance Disposal Technology Division (NAVEODTECHDIV) exploits technology and intelligence to develop and deliver EOD information, tools, equipment, and their life cycle support to meet the needs of joint service EOD operating forces and other customers. Its core functions are—

- Developing EOD procedures to counter munitions threats.
- Developing tools and equipment to meet EOD operational needs.
- Performing in-service engineering for EOD tools and equipment.
- Performing depot-level management and repair for EOD tools and equipment.
- Maintaining an EOD explosive hazard database.

RAPID EQUIPPING FORCE

5-32. The Rapid Equipping Force (REF) is an organization that takes its operational guidance from the Assistant Chief of Staff, Operations and Plans (G-3) and reports directly to the vice Chief of Staff of the Army. It has a broad mission to rapidly increase mission capability while reducing the risk to Soldiers, Marines, and others. The REF accomplishes this mission in the following three ways:

- Equips operational commanders with off-the-shelf (government or commercial) solutions or near-term developmental items that can be researched, developed, and acquired quickly.
- Inserts future force technology solutions that our engaged and deploying forces require. It does this by developing, testing, and evaluating key technologies and systems under operational conditions.
- Assesses the capabilities and advising Army stakeholders of the findings that will enable our forces to rapidly confront an adaptive enemy.

TECHNICAL ESCORT UNITS

5-33. The technical escort units will, on order, deploy task-organized teams to the continental United States (CONUS) or outside the continental United States (OCONUS) to conduct technical escort, CBRN hazard characterization, monitoring, disablement, and elimination support operations. They provide WMD and CBRN incident emergency response, homeland defense, and contingency support operations to combatant commanders and lead federal agencies. They also provide site remediation and restoration support operations for DOD.

TECHNICAL SUPPORT WORKING GROUP

5-34. The Technical Support Working Group (TSWG) is the United States national forum that identifies, prioritizes, and coordinates interagency and international research and development (R&D) requirements for combating terrorism. The TSWG rapidly develops technologies and equipment to meet the high priority needs of combating the terrorism community (to include IEDs) and addresses joint international operational requirements through cooperative R&D with major allies.

5-35. Since 1986, the TSWG has pursued combating terrorism technologies in the broad context of national security by providing a cohesive interagency forum to define user-based technical requirements spanning the federal interagency community. By harnessing the creative spirit of the U.S. and foreign

industry, academic institutions, government, and private laboratories, the TSWG ensures a robust forum for technical solutions to the most pressing counterterrorism requirements. Participants in the ten functional subgroup areas of the TSWG can come to a single table to articulate specific threats and a user-defined approach to the rapid prototyping and development of combating terrorism devices, training tools, reference materials, software, and other equipment.

5-36. The TSWG continues to focus its program development efforts to balance investments across the four pillars of combating terrorism. They include—

- **Antiterrorism.** Antiterrorism is the defense measures taken to reduce vulnerability to terrorist acts.
- **Counterterrorism.** Counterterrorism is the offensive measures taken to prevent, deter, and respond to terrorism.
- **Intelligence support.** Intelligence support is the collection and dissemination of terrorism-related information taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of CBRN materials or high-yield explosive devices.
- **Consequence management.** Consequence management is the preparation and response to the consequences of a terrorist event.

UNITED STATES AIR FORCE PROTECTION BATTLE LABORATORY

5-37. The United States Air Force Protection Battle Laboratory identifies innovative concepts for advancing joint warfighting. It uses field ingenuity, modeling, simulation, and actual employment of exploratory capabilities in OEs to test new and innovative ideas which can be readily transitioned into the FP arena.

UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND

5-38. The United States Army Intelligence and Security Command (INSCOM) conducts dominant intelligence, security, and IO for military commanders and national decision makers. Charged with providing warfighters the seamless intelligence needed to understand the battlefield and to focus and leverage combat power, INSCOM collects intelligence information in all intelligence disciplines. INSCOM also conducts a wide range of production activities, ranging from IPB to situation development, signal intelligence analysis, imagery exploitation, and science and technology intelligence production. INSCOM also has major responsibilities in the areas of counterintelligence (CI) and FP, electronic and IW, and support to force modernization and training.

5-39. INSCOM is a global command with four brigades that tailor their support to the specific needs of different theaters. Eight other groups or activities located worldwide focus primarily on a single intelligence discipline or function. They are available in a reinforcing role, enabling any combat commander to use INSCOMs full range of unique capabilities.

UNITED STATES ARMY MATERIEL COMMAND

5-40. The United States Army Materiel Command (USAMC) shares responsibility for managing the overt acquisition of foreign materiel for TECHINT purposes. The USAMC buys foreign materiel for exploitation purposes in the United States, as well as through its centers in Europe and the Far East.

UNITED STATES MARINE CORPS WARFIGHTING LABORATORY

5-41. The United States Marine Corps Warfighting Laboratory (MCWL) is the lead United States Marine Corps (USMC) agency for IED defeat. MCWL leads a USMC IED working group made up of representatives from the USMC, beltway agencies, and operating forces. The USMC IED working group works to rapidly identify, evaluate, and facilitate the fielding of materiel and nonmateriel counter-IED

solutions to the operating forces. They work in close coordination with the JIEDD TF/integrated product team (IPT) to synchronize DOD IED defeat efforts.

WEAPONS INTELLIGENCE DETACHMENT

5-42. The Weapons Intelligence Detachment is deployed at brigade level. They assist with IED incidents.

Chapter 6

Improvised Explosive Device Responses

The use of IEDs on the modern battlefield has a direct impact on mobility, survivability, and logistical support requirements. All units must be able to maintain operations despite these hazards. Units must understand what actions to take upon encountering a suspected IED. The following are the keys to success:

- **Adaptation.** The enemy will continue to adapt, and units must adapt also.
- **Information flow.** Share information.
- **Training.** Training is a must, even as a unit is deployed.
- **After-action reviews.** Conduct honest, thorough after-action reviews (AARs) after every mission.

COMMANDER'S GUIDANCE AND AUTHORIZATION

6-1. Commanders receive guidance or authorization from higher HQ in an operation order (OPORD) or established procedures in the unit SOPs that frame IED responsibilities during operations. While every unit must send an explosive hazard spot report when encountering an IED, a commander must decide whether to mark and bypass the IED, isolate the area for follow-on EOD neutralization, or remotely destroy the device. The EOD team is a combat multiplier to any operation and is the only organization authorized and equipped to conduct render safe neutralization of an IED and collect detailed forensics from it. Before a commander decides to destroy IEDs with organic assets, he must weigh the mission requirements with both safety and potential actionable intelligence. Destroying the IED is extremely dangerous and the less desirable COA due to unforeseen considerations in the construction and placement of the IED and potential secondary IED arrangement. Additionally, destruction most likely will prevent forensic analysis that provides intelligence to interrupt the IED supply chain and decision cycle of the enemy, which may impact IED use in the future.

WARNING

If the IED is suspected to have chemical, biological, or radiological (CBR) components, it is an imminent CBR threat. Take appropriate protective actions, and report it immediately.

LEADER'S DECISION CONSIDERATIONS

6-2. When a unit encounters a suspected IED, the leader must make a decision on the appropriate action to take. After taking immediate actions to alert personnel and remotely confirm the suspected IED, the leader must assess the following operational, situational, and tactical factors:

- The effect of the delay on the mission.
- The threat from direct and indirect fire. The risk of casualties from direct or indirect fire may be greater than that from the IED.
- The size and location of the IED.
- The type of terrain. The terrain determines the effectiveness and discernibility of the IED and, consequently, the ability of the unit to detect, avoid, neutralize, or protect against it.

- The alternate routes or positions available.
- The location and security of potential ICPs.
- The degree of protection available.
- The capabilities of the unit.
- The availability of EOD support.
- The dedicated security support for EOD.
- The danger to follow-on forces and missions.
- The danger to the civilian population and infrastructure.

6-3. After assessing the situation, the leader must report it according to the unit SOP. An example of a leader's decision considerations is outlined in Figure 6-1. Possible leader COAs include—

- Marking and bypassing the IED.
- Isolating and securing the area for EOD neutralization and collection and analysis of actionable intelligence.
- Remotely destroying the device.

ACTIONS WHEN SAFETY OR INTELLIGENCE IS THE PRIORITY

6-4. All service personnel (Army, Navy, Air Force, Marine, DOD civilians, and contractors) are responsible for the immediate actions required to react to IEDs.

6-5. If a suspected IED is found, the following basic confirm, clear, call, cordon, and control (5-Cs) steps will help to ensure that the situation is dealt with quickly and safely. Remember, the first 5 to 10 seconds are critical. Your response must be instinctive and effective.

6-6. The commander should conduct the 5-Cs and then wait for EOD personnel to neutralize the device. While waiting, the commander should ensure that appropriate protective measures are taken to minimize the risk to personnel and equipment. He can choose to evacuate, isolate, or protect against the effects of the IED, depending on METT-TC.

CONFIRM

6-7. The presence of the suspected IED should be confirmed. This should be done from a safe distance whenever possible. Maximum use of hard cover and spotting equipment (binoculars and scopes) should be made. From your position, conduct 5- and 25-meter checks to ensure that no secondary devices are present. When in convoys, the first vehicle to identify an IED should turn on the appropriate turn signal indicating contact and use a unit-designated IED marking system. The nearest vehicle (outside of 100 meters from the IED) with a radio must transmit the location of the IED to the remainder of the convoy using vehicle interval call signs and indicate the distance and direction of the threat (for example, "This is vehicle 4, possible IED, 3 o'clock 50 meters").

CLEAR

6-8. The area around the device should be cleared. All leaders must take immediate action to halt or reposition a minimum of 300 meters from the IED site. Detonation may be imminent if the device was activated before being located. When there is a possibility that all IEDs have not been located, stay alert. Once the unit clears the minimum 300-meter safe distance from the suspected IED, either the lead or trail security element will conduct a 25- to 50-meter sweep on each side of the route to locate IED materials and equipment (detonating cord, receivers, transmitters, and so forth) that may lead to other IEDs flanking the unit. If subsequent IEDs are located, units will execute the procedures for clearing the area as listed above.

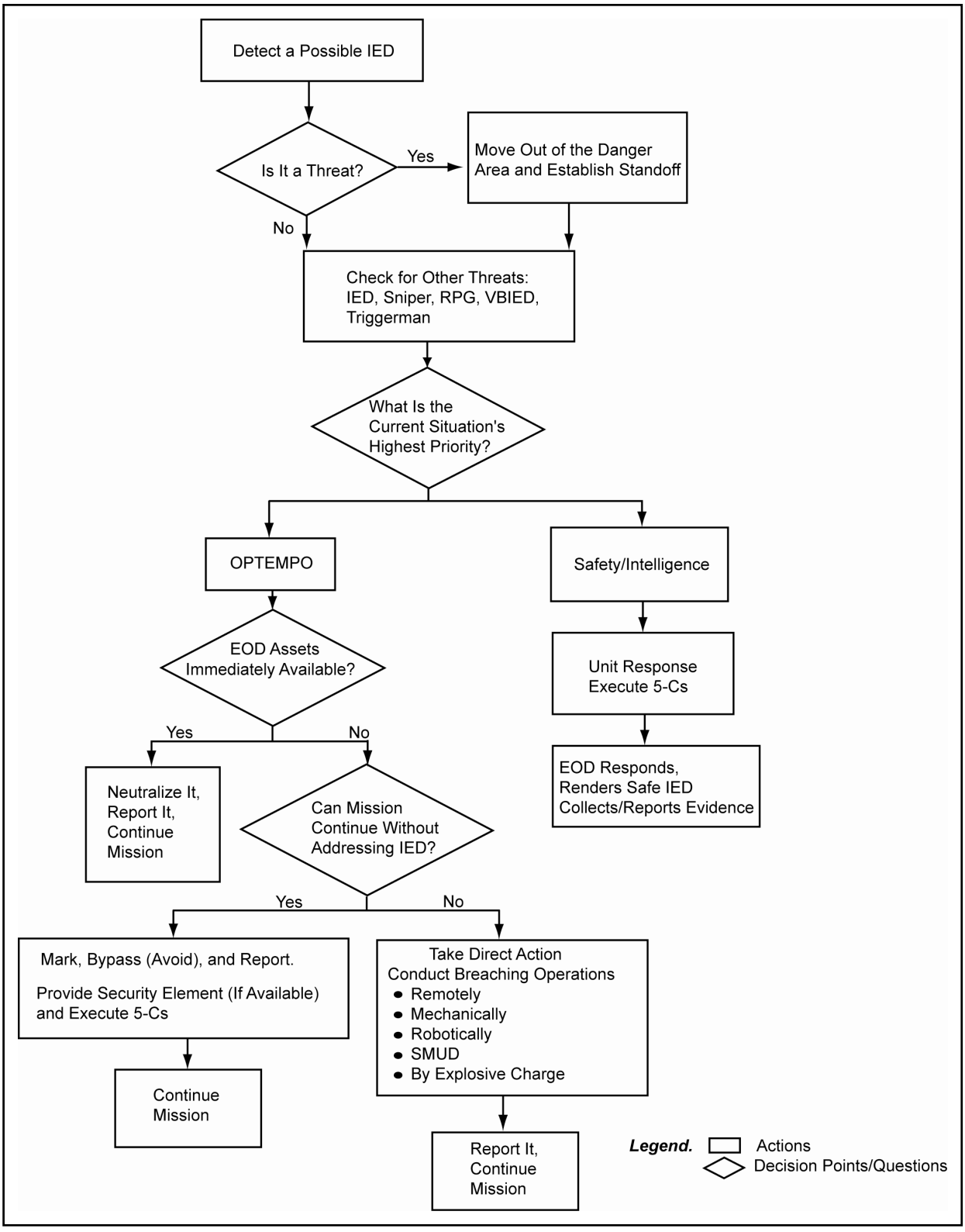

Figure 6-1. Sample of leader's decision considerations

6-9. Personnel should be cleared from the area. Injured personnel caught in the kill zone should be immediately extracted in a controlled and safe manner. Uninjured personnel should avoid the kill zone and be evacuated to a safe distance. A deliberate check of all personnel should be conducted in an effort to determine potential suspects related to the IED when clearing personnel out of the area. Suspects should be detained as defined by the current rules of engagement (ROE).

CALL

6-10. The suspected IED device should be called in as soon as possible. After leadership confirms the presence of a suspected IED, they immediately report according to the unit SOP using the 9-line explosive hazard spot report format described in Appendix D.

CORDON

6-11. The area should be cordoned off (a minimum of 300 meters from a small device, 1,000 meters for a van-sized device, and 2,000 meters for a truck-sized device). The purpose of the cordon is to prevent unauthorized personnel from entering the site (for their own safety and for the safety of the EOD responders), to preserve the scene for further exploitation, and to provide outward protection and security against command-initiated IEDs. A cordon force, whose form will depend on available assets, mans the perimeter. Around any area where you would set up a perimeter, check for secondary IEDs.

CONTROL

6-12. To ensure only authorized access, control the area inside the cordon. Only emergency services (medical, firefighting, or EOD) should be allowed to enter the cordon. All civilian traffic should be diverted away from the cordon. To ensure that no tampering occurs, maintain (from a safe distance) a visual/line-of-sight (binoculars and scopes) observation on the IED. Immediately report any personnel observed approaching the IED according to the unit SOP. A 360° security around the cordon should be maintained until EOD has given the all-clear signal.

6-13. For follow-on agencies, set up an ICP. The senior leader on the ground should maintain control of the site until the EOD assets arrive. The EOD team leader will take charge of addressing the IED and may request the senior leader to adjust the perimeter. Change of ownership (such as site control) may or may not occur at this point.

6-14. The military incident commander has C2 of the overall EOD incident a suspect device has been found. The incident commander will coordinate the operation with technical advice from the EOD team leader and supporting agencies.

6-15. Upon arrival, the EOD team leader has control of the incident site within the cordon around the IED and is responsible for observing all safety procedures for equipment and explosives used. Control of entry into the cordon area during an IED operation is approved only by the EOD team leader, who will direct all actions within the cordon. Actions include coordination of incident site exploitation and searches and direction of specific uses of CREW (counter radio-controlled improvised explosive device [RCIED] electronic warfare) equipment. To prevent fratricide, the EOD team leader must have control of all CREW assets operating in the area.

6-16. EOD team leaders will maintain a close liaison with the incident commander to ensure that correct security, search, EOD, and CREW procedures are executed within the bounds of safety and tactical considerations. The EOD team leader is responsible for the RSP and, as such, must be involved in every aspect of incident planning. The EOD team leader will coordinate all safety aspects through the incident commander and directly coordinate the use of CREW. The EOD team leader will notify the incident commander upon completion of the EOD mission.

PROTECTIVE MEASURES

6-17. Consider the information in the paragraphs below when evacuating, isolating, and barricading an area.

Evacuate

6-18. Evacuation of personnel and equipment is the best protective measure. Evacuate out to a minimum distance of 300 meters to reduce the hazard to personnel and equipment. If barricades (such as buildings) or natural terrain around the IED will absorb or deflect fragmentation and blast, these distances can be reduced. After all personnel and equipment are evacuated, movement within the area should be limited to essential operations only. Minimum evacuation distances are intended to be used for initial evacuation purposes only. In many cases, fragmentation will travel beyond these distances.

DANGER

If you can see the IED, it can kill you.

Isolate

6-19. When METT-TC allows, the senior leader may choose to isolate personnel and equipment from the IED area. Typically, isolation is used when the unit cannot build protective works around facilities or equipment that is unable to be evacuated. Do not build protective works around the IED. Natural or man-made terrain features are normally used to isolate assets from the IED.

Barricade

6-20. Equipment that cannot be moved must be protected from the effects of the IED with protective works. Personnel deemed to be mission essential must also be protected from the effects of the IED by reinforcing the fighting positions on the side facing the IED and by adding overhead cover. A protective work is an artificial barrier placed around key and essential equipment, personnel, or structures that provides limited protection by channeling the blast and fragmentation from the threatened area, thus reducing the effects of the blast and reducing the size of the evacuation area. The leader must be aware, however, that establishing protective works is very time and resource consuming.

6-21. Protective works can be fabricated from sandbags or earthmoving equipment and can be used when feasible. Do not barricade the IED itself. See FM 21-16/MCWP 3-17.3 for general guidelines on building, placement, size, and types of protective works.

EXPLOSIVE ORDNANCE DISPOSAL RESPONSE

6-22. The role of the EOD company is to support the leader and execute its assigned missions. EOD works in conjunction with engineer, MI, and other staffs to support the operational plan of the maneuver leader. EOD companies may be used to provide positive IED identification and safety guidance, perform render safe or disposal procedures, perform post blast, and perform crater analysis. EOD teams must have a dedicated security force. Teams can respond in a timely manner with dedicated security provided by the supported unit. Units can expedite the response of EOD teams by reporting accurate information on the 9-line explosive hazard spot report. Proper ordnance description or IED identification is instrumental in determining which types of equipment the EOD teams will need to neutralize the device.

Note. EOD personnel have specialized capabilities. Proper coordination and planning by the EOD staff cell is imperative to employ these capabilities at the right time and place on the battlefield. See FM 4-30.5, FM 21-16/MCWP 3-17.3, and FMI 4-30.5 for more information on EOD capabilities.

ACTIONS WHEN OPERATIONS TEMPO IS THE HIGHEST PRIORITY

6-23. When the unit is time-constrained to accomplish its mission (in the attack, conducting shaping operations, and so forth), possesses breaching capability, has no EOD assets readily available, the commander may be willing to accept risk of casualties (reduce safety) and in the attempt to neutralize the IED internally, METT-TC will dictate. If engineer or EOCA personnel are present, they can advise and assist. Techniques, in order of preference (for safety and FP), include—

- **Marking and bypassing.** SU, good communications, and prior planning will allow the force to best use this technique. The leader may employ preplanned alternate tactical plans according to the current OPORD.
- **Mechanical breaching.** Employment of mechanical reduction assets (vehicles or equipment) for breaching obstacles.
- **Remote or robotic neutralization.** Small robotic systems can be used to provide Soldiers and Marines with a standoff capability to keep personnel outside the blast radius. The robot may employ a weapons system or an explosive charge to neutralize an IED. Remotely-operated laser systems are a viable method of standoff IED neutralization.
- **Standoff munitions disruption.** Standoff munitions disruption (SMUD) is remotely detonating, disrupting, or deflagrating small ordnance at safe distances. Systems used to SMUD include the Barrett .50 caliber, 7.62 millimeter, and 5.56 millimeter rifles.

WARNING

Use of SMUD techniques can leave a fully functional IED or other explosive hazard. It is difficult to verify that the hazard has been neutralized.

- **Explosive charge.** Setting an explosive charge with a delay fuze near the IED is an alternative to the SMUD technique, particularly where a downrange hazard might not allow the shooting of projectiles. The charge should be remotely or mechanically emplaced using robots or a vehicle with a hydraulic arm (such as the Buffalo).

WARNING

An IED in the open may be a detonator for a larger hidden device. Ensure that there is enough safety stand-off distance from the IED before detonating it.

MILITARY SEARCH

6-24. Combating the enemy is not easy. In general, the enemy holds the initiative and our forces have to react to its activities. In all operations, it is vital to deprive the enemy of munitions and other material that may be used against military forces or the civilian populace. One of the best techniques for doing so is the military search, which is one of the few operations where the security forces have the initiative (being able to decide when, where, and how the operation will take place).

6-25. Military search is the management and application of systematic procedures and the appropriate detection equipment to locate specified targets. The aim of military search is to assist in the defeat of an enemy who uses terror tactics. The general search objectives include—

- Depriving the enemy of resources.
- Protecting potential targets.

- Gaining intelligence.
- Gathering forensic evidence.

6-26. All search operations should be driven by strong intelligence and have clearly defined objectives that contribute to the military mission. The political and social effects of any intended search operation should be addressed when considering the objectives.

6-27. Before conducting planning for search operations, it is essential to be absolutely clear about the objective of every search operation. METT-TC will assist in determining the search method, and the number and type of search teams involved. The speed at which the operation can be conducted is always governed by the aim and objectives of the search. Some typical examples include—

- Finding an enemy hide (a space in which resources are concealed) for munitions and equipment.
- Searching for suspected enemy IEDs.
- Finding and assisting in the clearance of IEDs from locations of importance to our forces.
- Allowing our forces to conduct offensive operations.
- Gaining intelligence (including tactical intelligence).
- Gaining forensic evidence in order to catch the enemy and have it convicted within the framework and conditions of the law in the HN.

6-28. Searching for IEDs is only part of the solution. Continued pressure must be applied and maintained in all areas through the use of patrols, surveillance, operations, and temporary traffic control points (TCPs).

WARNING

Routines should be varied, and do not develop patterns. Patterns are allowing the killing of Soldiers and Marines. Developing patterns gives the enemy what it is looking for—a time and a place.

ROUTE CLEARANCE OPERATIONS

6-29. The purpose of route clearance is to eliminate concealment for IEDs and munitions caches and the systemic detection and deterrence sweeps along the cleared routes. Clearance teams should be comprised of—

- Mechanized and combat heavy engineers.
- EOD teams (while not task-organized as part of the clearance company) who will respond promptly to route clearance teams' calls for assistance. Upon receipt of request for assistance (using the 9-line explosive hazard report) and in conjunction with dedicated security elements, EOD teams will respond according to the commander's priorities of effort, to render safe and dispose of IEDs in their AO. EOD response priorities include safety, collection of actionable intelligence in order to target the bomb maker, and contribution to assured mobility of routes.
- EOCA personnel, who are task-organized in route clearance operations, can remotely identify and dispose of by detonation only those designated UXO for which they are specifically trained and authorized. EOCA personnel are not trained or authorized to render safe and/or dispose of IEDs.

6-30. Route clearance missions consist of the following two phases:

- Right-of-way clearance.
- Route maintenance and sweep operations.

RIGHT-OF-WAY CLEARANCE

6-31. Units should remove rubble, debris, berms, holes, trenches, vegetation, and trash from the medians and shoulders of MSRs in order to eliminate concealment of IEDs and munitions caches and to aid in the

visual and sensory detection of IEDs. Units should then conduct a deliberate route reconnaissance, identify and record the location of man-made objects (buried pipe and cable), and investigate suspicious areas.

ROUTE MAINTENANCE AND SWEEP OPERATIONS

6-32. The unit should conduct systemic, random detection sweeps of the cleared areas and progress to detection and deterrence sweeps along the cleared route. A visual detection sweep should focus on changed conditions. Any investigation of suspected devices will be performed remotely with the Buffalo or other system, as required. The preferred way to conduct route clearance is to form C2, detection, security, and improvement elements.

Command and Control Element

6-33. The C2 element integrates the activities of the security, detection, and improvement sections. It maintains communications with its higher HQ and with the maneuver unit whose battlespace the clearance unit is operating in. The C2 element usually travels within the security element.

Detection Element

6-34. The mission of the detection element (Figure 6-2) is to scan the medians and shoulders of a route before employing engineer equipment to remove concealment and obstacles. The element will sweep the median and shoulder for IEDs, UXO, and mines; investigate all suspicious objects; mark and report UXO; and secure and report IEDs. When a suspected object is detected, the location will be pinpointed. The suspected object will be investigated remotely. EOD is the only force authorized to render safe an IED.

Note. Do not attempt to render safe, disassemble, or dispose of a suspected or actual IED during route clearance operations. For IED search and detection principles, see Appendix F.

Figure 6-2. Detection element

Security Element

6-35. The security element (Figure 6-3) consists of the forward, flank, and rear sections. The mission of the security element is to provide traffic control, crew-served weapons support, and FP and can dismount as necessary. The mission of the forward security section is to observe oncoming traffic for threats, identify hazards or obstructions in the route, and contain suspect vehicles identified by other elements. The mission of the flank security section is to protect the main body from threats on the shoulder or from traffic traveling in the opposite direction, observe vehicles passing through the work area for threats, and provide traffic control within the work area. The mission of the rear security section is to observe traffic approaching for threats, provide a visual warning to traffic that the clearance unit is ahead on the road,

contain suspect vehicles, and provide limited traffic control. The three security teams must be integrated and centrally controlled.

Figure 6-3. Security element

Improvement Element

6-36. The mission of the improvement element (Figure 6-4) is to remove all concealment for IEDs from the entire width of the median and from the shoulders of the road to a minimum distance of 25 feet. The best package for the improvement element is two bulldozers, two scrapers, a bucket loader, and a 20-ton dump truck. Upon completion of the work of the improvement element on a section of the route, the median and shoulders should be flat and level, eliminating any opportunity to hide IEDs or IED-making material without altering the terrain. Given random, systemic detection sweeps, changes in terrain will become immediately obvious, indicating potential IEDs.

Figure 6-4. Improvement element

6-37. Based on the terrain and the equipment available in the improvement element, leaders can expect the rates of march during clearing operations as shown in Table 6-1, page 6-10.

Table 6-1. Rate of march during clearance operation

Vegetation	*Two Dozers*	*Two Dozers, Two Scrapers, One Bucket Loader, and One 20-Ton Dump Truck*
Light	3 km/day	10 km/day
Moderate	2 km/day	8 km/day
Heavy	1 km/day	4 km/day

6-38. Figure 6-5 depicts the standard organization for a clearance operation.

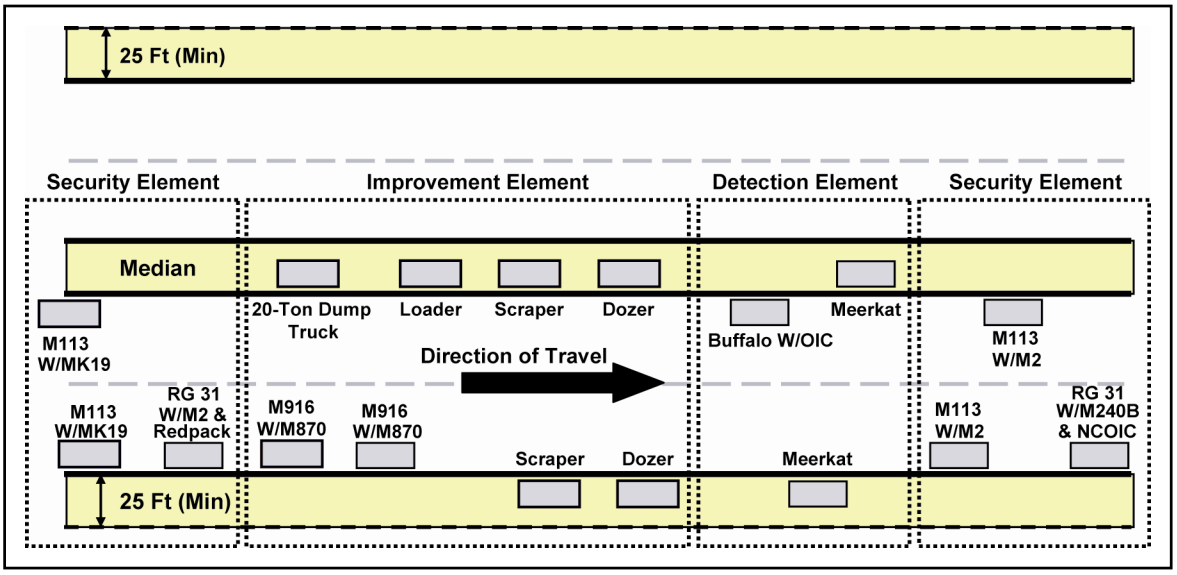

Figure 6-5. Standard organization for route clearance operation

Chapter 7

Improvised Explosive Device Defeat Planning Considerations

The METT-TC factors are the variables whose infinite mutations always combine to form a new tactical pattern. They never produce exactly the same situation; thus, there can be no checklist that adequately addresses all the situations. Each tactical problem is unique and must be solved on its own merits. This chapter provides an overview of the planning processes of the Army and describes how the commander and staff integrate IED defeat considerations into unit plans. Additionally, it discusses IPB, targeting, and risk management as additional tools to assist the commander and staff in integrating IED defeat considerations. This chapter also offers planning considerations for IED defeat based on the METT-TC factors. The factors for the considerations are not all-inclusive, but serve as a base for further development depending on the situation. Appendix B provides a detailed discussion of IED-defeat related considerations during an IPB.

SECTION I – PLANNING PROCESSES

7-1. As described in Chapter 1, IED defeat operations are part of the broader mission of the unit to predict, detect, prevent, avoid, neutralize, and protect the force from IED attacks. IED defeat considerations cut across the BOS and are not tied specifically to a staff cell or type of unit.

7-2. Means of integrating IED defeat considerations are the two tactical planning processes of the Army: the military decision-making process (MDMP) and troop-leading procedures (TLP). The MDMP is more appropriate for HQ with staffs. It provides a logical sequence of interactions and decisions between the command and staff for developing estimates and effective plans and orders. At lower tactical echelons, commanders use TLP to plan and prepare for an operation (see FM 5-0). Both planning processes provide a logical sequence of understanding the situation, developing and analyzing the COA, deciding on the best COA, and producing a plan or order to accomplish the mission.

7-3. During the MDMP, commanders play a critical role in planning. After receiving a mission, commanders develop their initial commander's visualization. They describe this visualization to the staff in the form of a commander's intent, a commander's planning guidance, and a commander's critical information requirement (CCIR). The staff then uses the commander's guidance to continue planning. IED defeat may have a large impact on a commander's planning guidance and the CCIR.

7-4. The goal of the MDMP is to achieve a faster decision cycle than the threat. Planning considerations for increased operational tempo and control of the battlespace will entail an aggressive mindset (become the hunter, not the hunted) and rapid responses to the IED threat, both operationally and technologically. If the threat responds to new technologies or procedures, then coalition forces must be able to also rapidly change TTP and technologies.

7-5. Threat centers of gravity must be identified and understood (identify who the bomb maker is at the tactical level). Data collection on IED characteristics and threat tactics place a "signature" on an IED that should be tracked and catalogued (identify who the financier is at the strategic level). The funding sources are identified, and this threat is addressed at the strategic level of warfare. All C2 assets and support infrastructure are leveraged to achieve a faster response time than the threat. The new capabilities needed are identified to overcome a dynamic, changing threat and get new TTP and capabilities into the field as

rapidly as possible. If impediments exist to rapid response in IED TTP or technologies, then identify the bottlenecks and raise the issues to the appropriate level of command to bypass or overcome the bottleneck. A more rapid decision and response cycle is the key to minimizing innovative threat IED practices.

7-6. IED defeat factors are considered throughout the planning process and are contained throughout the OPORD of the unit. Information, directives, and tasks for IED defeat may be found in several parts of the OPORD of the unit. For example, enemy information concerning IED attacks may be found in Annex B (Intelligence) and Annex F (Engineer). Specific tasks, such as "Conduct a Raid to Destroy a Bomb-Making Factory," may be found in tasks to subordinate units in the base OPORD. High-payoff targets related to IED defeat may be found in Annex B (Intelligence) and Annex D (Fire Support). Specific instructions on neutralization and disposal of IEDs may be found in Appendix 5 (Explosive Ordnance Disposal) to Annex F (Engineer) of the OPORD (see FM 5-0).

7-7. In other instances, IED defeat may be the focus of the entire unit OPORD. For example, an infantry company conducting a raid to seize a weapons cache or an engineer unit assigned a route clearance mission.

7-8. In addition to the MDMP and TLP, there are other staff processes designed to assist the commander and staff in synchronizing operations. These include—

- IPB (see FM 34-130).
- Targeting (see FM 6-20-10).
- Risk management (see FM 100-14).

These processes are continuous throughout the operations process (plan, prepare, execute, and assess) and aid with integrating IED defeat considerations into unit operations.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

7-9. IPB is the systematic, continuous process of analyzing the threat and environment in a specific geographic area. IPB is designed to support the staff estimate and MDMP. Most intelligence requirements are generated as a result of the IPB process and its interrelation with the MDMP (see FM 34-130). IPB products support the commander and staff and are essential to estimates, planning, targeting, and decision making.

7-10. The G-2/intelligence staff officer (S-2) leads the staff through the IPB process. Staff officers must assist the G-2/S-2 in developing IPB products, to include the situational template (SITTEMP) within their own areas of expertise or functional area. IPB starts during mission analysis, is refined during the rest of the MDMP, and continues during the preparation and execution of operations. IPB consists of the following four steps:

- **Step 1.** Define the operational (battlefield) environment.
- **Step 2.** Describe the battlefield effects on operations.
- **Step 3.** Determine threat models.
- **Step 4.** Determine enemy COA.

7-11. Geospatial considerations are a key aspect of IPB. Topographic engineer assets are employed to represent the threat geospatially. Pattern analysis and terrain analysis should be used to support a more rapid operational tempo than threat forces. The following geospatial factors and practices should be considered when planning:

- Track IED incidents and represent them geospatially. Ideally, categorize, map, and analyze every IED after it has been detonated to show pattern analysis that can lead to a better understanding of threat practices.
- Track the technologies used (flying IED versus buried IED, shaped charge versus blast/fragmentation, and so forth), and represent them geospatially to convey an operational understanding of threat IED use.
- Categorize and map the bomb-makers "signature" (technology used, tactics used, and so forth).
- Map out IED density with the location, dates, and frequency.

- Filter out "white noise" IEDs from mass casualty IEDs. (White noise IEDs are quickly employed and hard to stop, but create less damage; mass casualty IEDs take longer to emplace and create more damage.) Display different IED types geospatially, with color-coded representation, to better convey knowledge to decision makers.
- Use microterrain where possible for line-of-sight analysis, to include fire points, observation points and distances, range fans for potential enemy IED employment, and rapid response by friendly forces.
- Identify ideal prestaging locations for engineer and EOD equipment and/or teams to achieve a rapid response.
- Identify ingress and egress routes to potential IED event sites for threat interdiction and friendly response COA analysis.
- Fuse IED information with other data, to include cultural inferences (such as friendly or hostile mosque and/or ethnic group), civil affairs (CA) data (sewer, utilities, transportation), and so forth.
- Map out HUMINT, such as a hostile leader who was detained at one location and resides at a different location. Build patterns that can be used to geospatially understand the flow of threat personnel, information, and weapons.
- Understand how the enemy thinks. Use geospatial tools to understand the potential threat TTP. (Which route is frequently used by coalition forces? What locations will provide good visibility of the route and give the triggerman enough standoff space to egress after the attack? What areas offer the best concealment for the IED? Is there a feature that could serve as an aiming point for IED detonation? Are there locations where the terrain would enhance the IED blast effects? Where can the IED be emplaced to destroy coalition forces but not injure civilians who are allied with the insurgency?)

7-12. IPB products include the modified combined-obstacle overlay (MCOO), enemy SITTEMPs, event templates, and the high-value target list (HVTL) and provide key information in building the COP. Appendix B provides specific IED defeat considerations during the IPB.

TARGETING

7-13. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, taking account of operational requirements and capabilities (JP 1-02). It is an integral part of Army operations. Based on the commander's targeting guidance and targeting objectives, the targeting team determines what targets to attack and how, where, and when to attack. It then assigns targets to systems best suited to achieve the desired effects. Targeting begins during planning and continues throughout the operations process. It is a mechanism for the commander and staff to use to continually update and refine the plan and assess the operations through a cyclical process.

7-14. The targeting process follows the functions of decide, detect, deliver, and assess (D3A) (see FM 6-20-10). The targeting team, represented by the entire staff, considers all options (lethal and nonlethal) to create the desired effect on the intended targets.

7-15. The targeting process is another means of integrating IED defeat into unit operations. Critical nodes within the IED attack system of the enemy can be identified and nominated as high-payoff targets. Examples include specific leaders, bomb makers, or munitions caches. Collection assets are then assigned, ranging from HUMINT, signals intelligence (SIGINT), and imagery intelligence (IMINT) to reconnaissance patrols. Options are developed to attack key enemy IED nodes or to counter enemy IED attack efforts.

7-16. SMEs from various in-theater organizations, such as CEXC, provide targeting data which aids the prioritization and selection of targets.

RISK MANAGEMENT

7-17. *Risk management* is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits (FM 100-14). Risk management is integrated into the MDMP (see FM 5-0), and continues throughout the operations process. Commanders and staffs assess risk whenever they identify hazards, regardless of type; they do not wait until a set point in a cycle.

7-18. Effective risk management can reduce the frequency of IED strikes and diminish the physical effects when they do occur. It is used to identify hazards, define risks, identify methods for control, and identify responsibilities for implementation. The risk-management process enables commanders and staffs to define acceptable risk levels and implement controls until risks are commensurate with the mission. Risk management is a five-step process. The steps are as follows:

- **Step 1.** Identify the hazards.
- **Step 2.** Assess the risk of each hazard.
- **Step 3.** Make risk decisions and develops controls.
- **Step 4.** Implement controls.
- **Step 5.** Supervise and evaluate.

IDENTIFY THE HAZARDS

7-19. This is often the most difficult part of risk management. An IED incident is the condition that results from the interactions of an IED, a catalyst (such as activation from a Soldier, Marine, or vehicle), and a common spatial relationship. These hazards are defined in terms of the types of IEDs (such as a package IED, a VBIED, or a suicide bomber), how a Soldier or Marine might encounter the hazard (dismounted or mounted and the type of vehicle), and the locations where encounters would be most likely.

ASSESS THE RISK OF EACH HAZARD

7-20. This requires determining the probability and effects of an IED strike. An effective risk assessment is critical for evaluating the combat effectiveness of a unit in an IED environment. Risk-assessment criteria are developed by using Table 7-1. A sample risk assessment is shown in Figure 7-1 and will be discussed further in this chapter.

Table 7-1. Risk assessment matrix

SEVERITY		***PROBABILITY***				
		Frequent (A)	***Likely (B)***	***Occasional (C)***	***Seldom (D)***	***Unlikely (E)***
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L

RISK ASSESSMENT

DIRECTIONS: To access the risk of each item, circle the appropriate value number. See the remarks section below for guidance on assessing the value of the items.

TRAINING (circle one):
1 Experience working in IED areas.
2 No experience working in IED areas, but have training.
3 No experience or training working in or around IED areas.

TYPE OF AREA (circle one):
1 Area known by friendly forces to be clear of IEDs.
2 Old confrontation line or suspected IED area.
3 Area known to have IEDs.

LIGHT AND WEATHER (circle one):
1 Daylight with clear weather.
2 Daylight with poor weather.
3 Darkness.

MISSION (circle one):
1 One that Soldiers and Marines have done before.
2 One that subordinate leaders have done before.
3 An unfamiliar type of mission.

ON OR OFF ROAD (circle one):
1 Approved division or corps route.
2 Paved road.
3 Unpaved road.
4 Cross-country.

SLEEP (circle one):
1 Six hours of sleep in the last 24 hours.
2 Four hours of sleep in last 24 hours.
3 Two hours of sleep in last 24 hours
4 Awake for more than 24 hours.

TYPE OF VEHICLES IN CONVOY (circle one):
1 Armored.
2 Mixed, armored vehicles leading.
3 Wheeled.
4 On foot.

AVAILABILITY OF IED INFORMATION (circle one):
1 Updated IED, area graphics in each vehicle.
2 Updated IED, area graphics in the lead vehicle or a reliable, knowledgeable guide is available.
3 No upgraded IED, area graphics are available.

GROUND COVER (circle one):
1 Dry, hard ground with short grass.
2 Dry, hard ground with long grass or vegetation.
3 Wet, muddy ground or snow less than 10 centimeters deep.
4 Snow more than 10 centimeters deep.

ROAD USE (circle one):
1 Heavy, tracked vehicles or trucks recently used the road.
2 Light, wheeled vehicles recently used the road.
3 No traffic observed on the road; some tire marks.
4 No traffic observed on the road; no tire marks.

REMARKS:

If the circled value numbers above total—

10-16. Continue mission. Keep following training and common sense rules that apply to working around IEDs.

17-24. Continue the mission. Ensure that leaders maintain positive control of Soldiers and Marines and that they stress safety and IED awareness when briefing.

25-35. Consider postponing the mission until better conditions are attained. If you must continue the mission, constantly stress IED awareness and safety. Ask higher HQ for engineer support to accomplish the mission. Conduct IED-awareness training.

Figure 7-1. Sample risk assessment

MAKE RISK DECISIONS AND DEVELOP CONTROLS

7-21. This step requires decision makers to identify actions that can reduce the probability and/or severity to acceptable levels. This may be accomplished by taking actions to reduce the probability of an IED encounter or by providing more protection to the Soldier, Marine, or materiel to reduce the severity of an IED strike. Often, it is a combination of the two. Examples of controls include—

- Closing routes.
- Allowing only certain types of vehicles on the routes.
- Increasing patrols in suspected IED areas.
- Increasing observation suspected IED areas.
- Increasing protection of hardening of positions, facilities, vehicles, and personnel.

IMPLEMENT THE CONTROLS

7-22. Leaders must apply the identified controls to reduce the probability and severity of an IED attack.

SUPERVISE AND EVALUATE

7-23. This step ensures that controls are implemented to standard. PCI checks, rehearsals, and leader presence is key.

RISK MANAGEMENT SUMMARY

7-24. The key to using risk management successfully is to employ it at each echelon—from the commander, through the tactical planner, to the Soldiers and Marines executing the mission. Each level identifies hazards, eliminates or reduces hazards as feasible, and communicates the residual hazards to the next lower echelon. As such, each echelon works as a filter to control unacceptable risks.

7-25. Training provides Soldiers and Marines with an understanding of equipment limitations and plays a critical role in the risk management process. The capabilities and limitations of Army systems are taken into consideration during the development of doctrine and TTP.

7-26. Risk management at the tactical planning level requires a thorough knowledge and awareness of the hazards and potential controls that can be employed. The planning process requires a methodical and disciplined technique to identify the hazards and develop appropriate controls for operating in an IED environment.

7-27. The execution level is the culminating point of risk management. It is where Soldiers, Marines, and leaders employ the systems provided to accomplish the mission. The amount of residual hazards remaining

after the filtering process from echelons above may well determine the success of risk management. The individual Soldier or Marine is the last element to control any residual hazards.

7-28. Optimizing the components of risk management at the tactical planning level is more challenging as emerging technology dependent systems bring more variables into the mission. While tactical intelligence is the key element in identifying IED-related hazards, technical knowledge is the key element in assessing the risks associated with IEDs. This knowledge assimilates the tactical intelligence with the capabilities of the equipment of the unit, the performance of enemy IEDs, and the protection provided to our Soldiers and Marines by their vehicles or personal protective equipment.

7-29. See the risk mitigation considerations in Appendix E.

RISK ASSESSMENT MATRIX

7-30. The risk assessment matrix (Table 7-1, page 7-4) combines severity and probability estimates to form a risk assessment for each threat. Use the risk assessment matrix to evaluate the acceptability of a risk and the level at which the decision on acceptability will be made. The matrix may also be used to prioritize resources, to resolve risks, or to standardize threat notification or response actions. Severity, probability, and risk assessment should be recorded to serve as a record of the analysis for future use.

RISK DEFINITIONS

7-31. The following describes each of the risk definitions:

- **E – Extremely high risk.** Loss of ability to accomplish the mission if threats occur during the mission. A frequent or likely probability of catastrophic loss (I/A or I/B) or frequent probability of critical loss (II/A) exists.
- **H – High risk.** Significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, or inability to complete the mission to standard if threats occur during the mission. Occasional to seldom probability of catastrophic loss (I/C or I/D) exists. A likely to occasional probability exists of a critical loss (II/B or II/C) occurring. Frequent probability of marginal loss (III/A) exists.
- **M – Moderate risk.** Expected degraded mission capabilities in terms of the required mission standard will have a reduced mission capability if threats occur during the mission. An unlikely probability of catastrophic loss (I/E) exists. Seldom a probability of a critical loss (II/D) exists. Marginal losses occur with a likely or occasional probability (III/B or III/C). A frequent probability of negligible loss (IV/A) exists.
- **L – Low risk.** Expected losses have little or no impact on accomplishing the mission. The probability of critical loss is unlikely (II/E), while that of marginal loss is seldom (III/D) or unlikely (III/E). The probability of a negligible loss is likely or unlikely (IV/B) through (IV/E).

RISK SEVERITY CATEGORIES

7-32. The following describes each of the risk severity categories (see paragraphs 7-33 and 7-34 for a further explanation):

- **Catastrophic (I).** Loss of ability to accomplish the mission or mission failure. Death or permanent disability. Loss of major or mission-critical system or equipment. Major property (facility) damage. Severe environmental damage. Mission-critical security failure. Unacceptable collateral damage.
- **Critical (II).** Significantly degraded mission capability, unit readiness, or personal disability. Extensive damage to equipment or systems. Significant damage to property or the environment. Security failure. Significant collateral damage.
- **Marginal (III).** Degraded mission capability or unit readiness. Minor damage to equipment or systems, property, or the environment. Injury or illness of personnel.

- **Negligible (IV).** Little or no adverse impact on mission capability. First aid or minor medical treatment. Slight equipment or system damage, but fully functional and serviceable. Little or no property or environmental damage.

PROBABILITY DEFINITIONS

7-33. Table 7-2 (see FM 3-100.12) outlines the probability definitions for the risk assessment matrix.

Table 7-2. Probability definitions

Element Exposed	*Definition*
FREQUENT (A) - Occurs Very Often, Continuously Experienced	
Single item	Occurs very often in service life. Expected to occur several times over the duration of a specific mission or operation.
Fleet or inventory of items	Occurs continuously during a specific mission or operations or over a service life.
Individual	Occurs very often. Expected to occur several times during the mission or operation.
All personnel exposed	Occurs continuously during a specific mission or operation.
LIKELY (B) - Occurs Several Times	
Single item	Occurs several times in service life. Expected to occur during a specific mission or operation.
Fleet or inventory of items	Occurs at a high rate, but experienced intermittently (regular intervals, generally often).
Individual	Occurs several times. Expected to occur during a mission or operation.
All personnel exposed	Occurs at a high rate, but is experienced intermittently.
OCCASIONAL (C) - Occurs Sporadically	
Single item	Occurs sometime in the service life. May occur about as often as not during a specific mission or operation.
Fleet or inventory of items	Occurs several times in the service life.
Individual	Occurs over a period of time. May occur several times during a specific mission or operation, but not often.
All personnel exposed	Occurs sporadically (irregularly, sparsely, or sometimes).
SELDOM (D) - Remotely Possible; Could Occur at Sometime	
Single item	Occurs in the service life, but only remotely possible. Not expected to occur during a specific mission or operation.
Fleet or inventory of items	Occurs as isolated incidents. Possible to occur sometime in the service life, but rarely. Usually does not occur.
Individual	Occurs as isolated incidents. Remotely possible, but not expected to occur during a specific mission or operation.
All personnel exposed	Occurs rarely within the exposed population as isolated incidents.
UNLIKELY (E) - Can Assume Will Not Occur, But Not Impossible	
Single item	Occurrence not impossible, but can assume that it will almost never occur in the service life. Can assume that it will not occur during a specific mission or operation.
Fleet or inventory of items	Occurs very rarely (almost never or improbable). Incidents may occur over the service life.
Individual	Occurrence not impossible, but may assume that it will not occur during a specific mission.
All personnel exposed	Occurs very rarely, but not impossible.

RISK MANAGEMENT RELATIONSHIP TO THE MILITARY DECISION-MAKING PROCESS AND TROOP-LEADING PROCEDURES

7-34. As mentioned earlier, risk management is not an add-on feature to the MDMP or TLP. It is a fully integrated element of planning and executing operations. The goal of integrating the process is to make risk management a routine part of planning and executing operational missions. Table 7-3 describes the risk management process as it is integrated into the MDMP; Table 7-4, page 7-10, shows the risk management process as it is integrated into TLP, more detailed discussion on risk management and key risk management terms can be found in FM 3-100.12, FM 100-14, and FM 5-0.

Table 7-3. Risk management actions integrated into the MDMP

Military Decision-Making Process	*Risk Management Steps*				
	Identify the Hazards	*Assess the Risk of Each Hazard*	*Make Risk Decisions and Develop Controls*	*Implement the Controls*	*Supervise and Evaluate*
1. Mission Receipt	X				
2. Mission analysis	X	X			
3. COA development	X	X	X		
4. COA analysis (war game)	X	X	X		
5. COA comparison			X		
6. COA approval			X		
7. Orders production				X	
8. Rehearsal	X	X	X	X	X
9. Execution and assessment	X	X	X	X	X

Table 7-4. Risk management actions integrated into the TLP

Troop-Leading Procedures	*Risk Management Steps*				
	Identify the Hazards	*Assess the Risk of Each Hazard*	*Develop Controls and Make Risk Decisions*	*Implement the Controls*	*Supervise and Evaluate*
1. Receive the mission	X				
Perform initial METT-TC analysis	X				
2. Issue the warning order	X				
3. Make a tentative plan	X	X			
Make an estimate of the situation	X	X			
Conduct a detailed mission analysis	X	X			
Develop a situation and COA for the—	X	X			
- Enemy situation (enemy COAs)	X	X			
- Terrain and weather (OAKOC)	X	X			
- Friendly situation (troops and time)	X	X			
- COAs (friendly)	X	X			
Analyze a COA (wargame)	X	X			
Compare the COAs			X		
Make a decision			X		
Expand selected COA into a tentative plan			X		
4. Initiate movement				X	
5. Reconnoiter				X	
6. Complete the plan				X	
7. Issue the order				X	
8. Supervise and refine the plan					X

SECTION II – PLANNING CONSIDERATIONS

7-35. A thorough mission analysis is crucial to planning. Both the process and the products of mission analysis help the commander and staff develop and refine their SU and develop effective plans. By having a thorough understanding the METT-TC factors, the commander and staff are better equipped to develop effective plans to accomplish the mission. The remainder of this section offers IED planning considerations along the METT-TC factors.

MISSION

7-36. The mission statement defines the who, what, when, where, and why of the operation. A thorough understanding of why the unit is conducting an operation provides the focus for planning. Commanders analyze a mission in terms of the intent of the two higher commanders and their concept of operations. They also consider the missions of adjacent units to understand their contributions in relation to their own unit.

7-37. During mission analysis, the staff identifies those specified and implied tasks necessary for the mission accomplishment, to include IED defeat tasks. IED defeat must be an integral part of unit operations, particularly those operations involving maneuver and mobility within the unit AO. Leaders must coordinate their IED defeat efforts with adjacent units and integrate them as necessary. Often, leaders will need to coordinate the use of theater-level assets and resources for use in IED defeat operations. IED defeat tasks may include—

- Reconnaissance (route, zone, area).
- Security patrols.
- Route security.
- Route clearance.
- Area security, to include defending critical sites and infrastructure.
- Raids.
- Cordon and search.
- Sniper operations.

ENEMY

7-38. Both conventional and unconventional forces may use IEDs. However, IEDs are often a weapon of choice for insurgents and terrorists due to imbalances in technology or numbers. IEDs allow them to strike without exposing themselves. This negates the advantages of conventional forces and allows the insurgent or terrorist to fight on its own terms. Conventional forces are often left to mitigate the effects of the device which impacts upon mission completion.

7-39. The defeat of IEDs will often require a more holistic and coordinated approach than merely focusing on the device itself. IED defeat must engage the entire system, to include public support, financing, supply, manufacturing, leadership, and the planning processes of the enemy. Figure 3-1, page 3-3, depicts key nodes and activities within an enemy IED system.

7-40. Enemy considerations include their disposition (organization, strength, location, and tactical mobility), doctrine and/or methods, vulnerabilities, and probable COAs. Focus areas include—

- Methods and TTP for initiation of IED.
- Common materials used.
- Favored targets.
- Patterns developed for the areas and location of IED attacks.
- Organization (cells, echeloned, and so forth).
- Supply sources.
- Safe house and safe areas (for the insurgents).
- Level of popular support (may vary across the AO).
- Communications means.
- Known or suspected funding sources.
- Known or suspected leadership.

TERRAIN AND WEATHER

7-41. Terrain and weather are natural conditions impacting both friendly and enemy operations.

TERRAIN

7-42. The terrain has a direct impact on the selection of objectives and locations for the placement of IEDs. The type of terrain will also impact on the effectiveness of IEDs or the protective measures of friendly forces. The natural and man-made terrain features not only affect maneuver and mobility in an operation, but can also mask the employment of IEDs. Terrain is analyzed from both the friendly and enemy perspectives using the observation and fields of fire, avenues of approach, key terrain, obstacles, and cover

and concealment (OAKOC) methodology (see FM 7-92). Typical locations for enemy IED emplacement include—

- Bridges and overpasses.
- Road and rail intersections.
- Places that force slowdowns and closer intervals on convoys, such as winding turns, unpaved surfaces, steep or sharp turns, narrow roadways, and choke points.
- Areas of dense civilian traffic or congestion.
- Culverts or tunnels.
- Terrain that provides overwatch.
- Terrain that offers cover or concealment for IEDs and initiators.
- Terrain used for marshalling personnel, equipment, and supplies.

WEATHER

7-43. Weather and the climate have direct and indirect effects on IEDs. The weather affects—

- The visibility of IEDs, initiators, and targets.
- The selection of emplacement for IEDs.
- The effectiveness of IEDs. For example, low and dense cloud cover may increase the blast effects of an IED. Temperature and moisture may cause failure to initiate or premature detonation.

TROOPS AND SUPPORT AVAILABLE

7-44. When given a mission, a leader does a troop-to-task analysis. This analysis of troops and support available includes the number, type, capabilities, and condition of available friendly troops and support. It also includes supplies and support available from joint, multinational, and interagency forces. Commanders consider available troops and support when analyzing whether they have enough resources to accomplish a mission.

7-45. The types of units and support that commanders should consider for IED defeat operations include—

- Intelligence support, to include HUMINT, SIGINT, IMINT, and CI.
- Reconnaissance assets, to include reconnaissance units, scouts, and unmanned aerial vehicles (UAVs).
- Engineer units and support, to include mobility augmentation companies, clearance companies, Sapper units, search teams, and specialized search dog teams.
- EOD units or personnel.
- Combat forces, to include maneuver and fire support units.
- Linguist support.
- CA support.
- Military police units.
- Psychological operations support.

TIME AVAILABLE

7-46. Leaders must take into account the ability of their unit and subordinate units to plan, prepare, and execute operations within the time available. The ability of the enemy to plan, prepare, execute, and react is also a function of time. Within IED defeat, many operations are time-sensitive. They include—

- Convoying route change detection.
- Responding to an IED incident (EOD render safe and disposal, forensics, and so forth).
- Targeting.
- Raiding an IED maker or factory.
- Seizing stockpiled caches.

CIVIL CONSIDERATIONS

7-47. Civil considerations impact operations throughout the entire spectrum of conflict and at all echelons. Civil considerations comprise the influence of man-made infrastructure, civilian institutions, and attitudes and activities of the civil leaders, populations, and organizations within an AO on the conduct of military operations. Leaders must consider the relationship between IED defeat operations and the effects and influences they have on the civilian populace. They must also consider the impact of enemy IED attacks on the populace. The six characteristics that comprise civil considerations (expressed by the acronym ASCOPE) are—

- **Areas.** Areas are the political boundaries, city districts, municipalities, trade routes, sociological and religious enclaves, agricultural and mining regions, trade routes, and so forth. Support for U.S. forces may vary between areas. Analysis may indicate which areas have an increased chance for encountering IED activity.
- **Structures.** Structures are the infrastructure (dams, bridges, power plants, warehouses, communications nodes) and religious or cultural areas (mosques, churches, libraries, hospitals). Control of key structures can protect populations from hardship or deny their use to the enemy. Some structures may be identified as targets for military action; others may be prohibited from targeting.
- **Capabilities.** Capabilities provide sustenance, key civic services, and resources to support military operations. Populations with access to basic sustenance and services are usually not prone to support insurgent terrorist or criminal activity.
- **Organizations.** Organizations are the nonmilitary groups or institutions within the AO that influence and interact with the populace, the force, and each other. Identification of influential organizations may assist in gaining the support of the population.
- **People.** People is the general term for nonmilitary personnel encountered by military forces whose actions and influence can affect the mission. The support of the population is critical to U.S. forces. Some enemy forces, such as insurgents, cannot operate without the support of the people.
- **Events.** Events are the routine, cyclical, planned, or spontaneous activities that significantly affect organizations, people, and military operations. Events may arouse tremendous emotion in the population and affect support for U.S. forces.

7-48. Other civil considerations are ensuring that tasks and methods are in place for the employment, cultural understanding, and interaction with the local population, nongovernment agencies, and contractors in support of stability and reconstruction operations. Shaping how the enemy thinks is the key element required for IED defeat at the beginning of the process. A decrease in IED activity in the AO over time should be seen if such an effort is synchronized throughout the theater of operations. Once the aspect of how the enemy thinks is understood, you may be able to shape its actions in your favor. Using your abilities and capabilities to win over the enemy is essential for IED reduction. Proper integration of humanitarian projects in each AO (at ground level) that meets the most important needs of the local leaders and population can help to establish friendships and/or alliances. Such actions can have a positive impact on IED defeat at its source. Some points of consideration, though not a conclusive list, include—

- **Planning a meeting with the local leaders.** Know when the next meeting with the local leaders is and know the intent. Know about the culture, language, and the pressing needs of the community in the AO. Know what questions to ask and what questions to anticipate. Determine who in the AO knows the most about the leader, his population, and culture and if this person is essential to the meeting. Identify other essential personnel required for the meeting.
- **Meeting the essential community requirements.** After meeting with the community leaders, decide how the units can help meet some of the essential requirements in the community in such a way as to help win over the population. For example, does this community require a trash service? Trash service, as our culture envisions, may not be what this local leader requires. His culture may desire that trash be removed to a specific site in order to attract wildlife that can be killed for food.

- **Improving formal and informal connections.** Formal and informal connections with the local population should be improved in a controlled manner, from the highest commander to the lowest level and tracking and assimilation of this information into the planning process should be ensured. This can include use of Special Forces, NGO, contractors, and interpreters; information obtained by employment; proper treatment of the local population on projects for their benefit and the benefit of the unit; establishment of business opportunities for local leaders and their community; and media considerations. For example, there may be an opportunity to create conditions for brass and plastic recycling during ammunition de-milling or to establish a local construction element for road improvement in the area that benefits local and military activities. Such activities are essential to decrease the IED production at the source, providing that the community needs are met and the information is shared with the local population in such a way as to convey good intent by the units.

Note. The perceived ability to attack and destroy IED enemy nodes contributes to success in stability and reconstruction operations by deterring potential threats. Conversely, successful stability and reconstruction operations reduce the chance of IED threat by influencing civilians to not support the enemy efforts.

SUMMARY

7-49. IED defeat considerations are incorporated into unit plans through the MDMP or TLP. Additional IPB, targeting, and risk management are other tools to assist commanders and staffs with IED defeat throughout the operations process. The IED planning considerations offered in this chapter serve as a guide for further development based on the situation.

Chapter 8
Training Requirements

Units must be prepared to perform IED defeat to serve in-theaters of operations around the world. Upon arrival to a theater, units are finding themselves performing operations traditionally reserved for combat arms units. With a clear lack of visible lines of contact, Soldiers and Marines are finding themselves constantly on guard and potentially performing combat arms tasks. Training at home stations before deployment is critical to ensure that units traditionally designated as CS and combat service support (CSS) can maneuver and survive on the battlefield. The information in this chapter will provide some necessary skills and information to be considered before deployment to a theater of operation.

OBSERVATIONS FROM THE FIELD

8-1. There is a significant tactical performance gap between unit predeployment training tasks, conditions, standards, and the actual tactical environment and mission expectations in-theater. Theater, FORSCOM, and TRADOC predeployment training guidance list tasks, but do not describe required capabilities. Units practice individual TTP, rather than execute a battle-focused wartime training strategy. Mandated certification of standardized tasks is driving a sequential, event-driven approach to predeployment training strategy, vice the battle-focused training strategies described in Army training doctrine.

8-2. Soldiers, Marines, and units transitioning for reception, staging, onward-movement, and integration (RSOI) report an expectation that they will be "trained" by someone before commitment to operations. This is particularly true for CS and CSS units. Some units with a high level of enemy attacks were found to have limited relevant training and low confidence in their own ability to fight effectively. They tend to look for a "silver bullet," such as SOPs, a text book TTP, or training from others outside their own leadership. Some units are assigned missions that are either different from their prewar mission (such as Multiple Launch Rocket System [MLRS] battalions performing military police battalion missions) or are executing missions under different conditions than prewar doctrinal assumptions (for example, there is no secure rear area).

8-3. The theater expects individuals and units that are trained to be ready to fight on arrival. There is neither time nor the resources to make up for predeployment training shortfalls during RSOI. The concepts of multiechelon training and the commander's responsibilities are essential to effective predeployment training. However, current operations have also shown that the conditions do not always match our established prewar doctrinal assumptions, training procedures, and exercises. For some combat arms units the difference is not great, requiring little adjustments. For many units, however, experiences in current operations have shown that prewar training techniques, resources, and assumptions have not prepared Soldiers, Marines, staffs, or leaders for the demands of combat. Training for current operations often means discarding or re-evaluating "the way we have always done it."

8-4. Basic expectations can be ascribed to any Army unit deployed to current operational theaters (combat, CS, CSS). Assessment of expectations and conditions in the current operational theaters have been synthesized down to this simple summary of tactical expectations, required techniques, required capabilities, training conditions, and enemy tactics. While it is infeasible to put every unit in the field at the highest collective levels or to recreate a combat training center (CTC)-like environment at every installation, it is not infeasible to train effectively and realistically. An effective predeployment training strategy to develop the right capabilities at the right levels is key. A commander (at any echelon) needs to

have confidence in the ability of his unit to meet expectations on arrival in-theater. The training strategy outlined in Tables 8-1 and 8-2, pages 8-4 through 8-7, show key skills, activities, and tasks that the leader and commander must see subordinates perform to standard. Demonstration of those skills requires prioritizing requirements for subordinates, allocating and providing the right resources, and the timing of the specific training exercises to cause subordinates to execute their responsibilities under relevant conditions.

8-5. Leaders need to apply tactical lessons learned to predeployment training and resource this training with personnel and equipment not organic to current modified tables of organization and equipment (MTOEs).

TRAINING EXPECTATIONS FROM THE FIELD

8-6. Paragraphs 8-7 through 8-11 refer to Table 8-1.

TACTICAL EXPECTATIONS

8-7. The column "Tactical Expectations" describes the tactical capabilities that theater missions, conditions, and threats demand of all units regardless of the type, function, or prewar doctrine. This does not replace unit functional requirements. For some combat arms, Soldiers, Marines, and unit expectations differ little from prewar doctrinal requirements. For many units, particularly CS, CSS, and units assigned nonstandard missions, these expectations are different from prewar doctrinal assumptions and training conditions. At the collective levels, expectations include shifting of tactical responsibilities, which under prewar doctrine belonged to the corps or division levels, down to lower levels of command for planning and execution.

TACTICAL TECHNIQUES REQUIRED

8-8. The column "Tactical Techniques" describes the skills that subordinates must train on in order to effectively meet the tactical expectations. For example, the conditions in-theater will require all Soldiers and Marines to participate in patrols. It does not matter whether this is an infantry Soldier or Marine participating in a reconnaissance patrol, an artilleryman participating in a combat patrol, or a CSS Soldier or Marine participating in a base security patrol. To meet the tactical expectation for Soldiers and Marines to be able to patrol, they must have been trained in these skills before deployment.

CAPABILITIES REQUIRED

8-9. The column "Required Capabilities" describes the required minimum personnel or materiel capabilities necessary for effective training, to include predeployment training. In many cases, these specialized personnel or additional equipment are part of a prewar MTOE of the unit or doctrinal expectations. Based on prewar doctrinal assumptions for many CS, CSS, and ARNG units, these items are either low-density items, not yet fielded, or not available for predeployment training. However, execution of operations, techniques, and threats may require these additional capabilities.

TRAINING CONDITIONS

8-10. The column "Training Conditions" requires leaders to assess readiness to meet tactical expectations. Realistic training conditions are essential to closing the gap between predeployment training and theater expectations. Conditions and standards that are published in doctrinal manuals and mission training plans (MTPs) may not be relevant to the expectations in-theater. For example, units experienced and conditioned by peacekeeping operations must be trained and conditioned for counterinsurgency operations because they are not the same. For most organizations, developing relevant, realistic training conditions requires reviewing and revising training resource allocations, peacetime range operations, and traditional branch or unit training strategies.

ENEMY TACTICS

8-11. The column "Enemy Tactics" describes the enemy tactics that Soldiers, Marines, and units must understand. Soldiers, Marines, and units require practice and experience applying the required tactical techniques and capabilities, under realistic conditions, for the focused purpose of defeating these enemy tactics and techniques. In training, opposing force (OPFOR) tactics are the most important aspect to emphasize. Specific techniques (types of IEDs, types of attacks) change very rapidly; however, enemy tactics (regardless of technique) typically remain relatively stable. Commanders must resist the temptation to chase the latest enemy technique during predeployment training and instead use enemy tactics to develop experience, adaptation, and aggressiveness in subordinates.

STAFF TRAINING

8-12. Commanders should ensure that staffs are properly trained to conduct planning as discussed in Chapter 7. Planning becomes an important process during IED defeat operations.

UNIT TRAINING

8-13. Unit training is a continuous process. Success comes from battle-focused training that emphasizes the training of essential warfighting tasks to standard. Units, leaders, and individuals train to standard on their assigned missions, first as an organic unit and then as an integrated component of a team. Their battle-focused training experience gives them the flexibility to continue training and adapting to the mission as it evolves.

8-14. The commander's responsibility is to focus on developing individual and collective training, not only mission-essential tasks. Visualizing the decisive effects is more important than simply listing all the MTP tasks and standards. The commander should—

- Establish the relationship between doctrinal concepts, unit mission-related priorities, and physical demonstration of proficiency.
- Describe the intent—visualization of desired arrangement of battlefield activities and the competencies required to achieve it.
- Establish personal measures for assessing organizational capability to meet requirements.
- Provide multiechelon training exercises that develop and assess appropriate leader, staff, and unit training.
- Arrange live-virtual-constructive (L-V-C) training to sustain proficiency and to expand an experience base for commanders, leaders, staffs, and units.
- Design and resource exercise evaluations (EXEVALs) and situational training exercises (STXs) to create opportunities to develop, observe, and assess combat proficiency.

8-15. Senior commanders use training evaluations as one component of a feedback system. To keep the training system dynamic, they use feedback to determine the effectiveness of the planning, execution, and assessment portions of the training management cycle. These feedback systems allow the senior commander to make changes that lead to superior training results and to teach, coach, and mentor subordinate leaders. To be effective, this feedback flows between senior and subordinate HQ, within each command echelon, and among a network of trainers that may cross several command lines. See Table 8-2, page 8-6, for a summary of suggested critical tasks for collective training.

Table 8-1. Training task list for training expectations from the field

				Individual Soldiers and Marines in all MOSs	*Tactical Leaders (commanders, staff officers and senior NCOs)*	*All Squad/Crew/Platoon in All Combined Arms Units*
Tactical Expectations	***Tactical Techniques Required***	***Capabilities Required***	***Training Conditions***	***Enemy Tactics***		
What do the missions, conditions, and threats dictate that all units must have the capability to perform?	What must commander's see their subordinates do in order to meet tactical expectations?	Additional nonstandard minimum capabilities required for effective training: organic/attached personnel or additional/new equipment fielding.	Must be trained and demonstrated under the following conditions:	Develop experience against the following threats:		
IED recognition Observation and reporting Individual patrol skills Actions on contact Urban movement - IMT and driving skills Physical fitness and endurance	Urban driving Close quarters marksmanship Mounted live fire Urban live fire TLP CLS and CASEVAC Observation and reporting Mounted land navigation	Detection optics Simple IED marking Reporting procedures Individual survivability equipment Individual communications equipment Night vision devices	IEDs Ambush Kidnapping Rocket/mortar/RPG Urban movement Theater culture Day/night operations	IEDs - RCIED IEDs - with DF ambush IEDs - combined with kidnapping IEDs - VBIED IEDs - with COB/HN forces Crowds restrict movement and fires Targeting of friendly patterns Drive-by shootings	Attack to recon U.S. responses IEDs - to isolate subunits IEDs - to distract/deceive IEDs - to cause casualties IEDs - to protect supplies/ workshops/leaders Intimidation of HN forces IED - with attack on responders False information from locals Mortar/rocket attacks on FOBs	IEDs - RCIED IEDs - with DF/ambush IEDs - with kidnapping IEDs - VBIED IEDs - with COB/HN forces Crowds to restrict movement/fires Targeting friendly patterns Drive-by shootings
Collect and process information Maintain offensive orientation Anticipate, prioritize, decide, adapt Delegate and multitask Disseminate information Organize and train subordinates Integrate new capabilities Lead forward Execute missions aggressively Execution	TLP Drive intelligence development "nonstandard" missions IO targeting Proactive decision making Create training strategies Perform actions on contact Persevere under pressure Analyze friendly and enemy patterns	Use of communications equipment Use of translators Use of pattern analysis tools Use of SU tools	Urban environment Decentralized operations Concurrent operations Simultaneous events "nondoctrinal" tasks IO targeting Negotiations Continuous stress Theater culture			
Secure site Secure movement Conduct actions on contact Conduct reconnaissance patrols Raid Cordon and search Ambush	IED recognition and reporting Urban driving and navigation CLS and CASEVAC CQM and mounted live fire LP Night operations TCP procedures ECP procedures Detainee procedures Vehicle/equipment recovery	Simple IED detection tools Simple IED marking tools Reporting procedures Survivability Communications	IEDs VBIEDs Mines/UXO Rockets/RPGs Mortars Sniper Ambush Kidnapping Urban movement Theater culture			

				Company Level	***Battalion and Brigade Levels***	***Division Level***
Tactical Expectations	***Tactical Techniques Required***	***Capabilities Required***	***Training Conditions***	***Enemy Tactics***		
What do the missions, conditions, and threats dictate that all units must have the capability to perform?	What must commander's see their subordinates do in order to meet tactical expectations?	Additional nonstandard minimum capabilities required for effective training: organic/attached personnel or additional/new equipment fielding.	Must be trained and demonstrated under the following conditions:	Develop experience against the following threats:		
Organize/execute site/base security Organize/execute convoy movements Organize/execute QRF Apply force discriminately Organize/execute reconnaissance patrols Consolidate after attack Perform CSS Integrate replacements Organize/execute raids and ambushes Organize/execute cordon and search	C2 TLP Report Integrate attachments Integrate into another unit Execute CASEVAC QRF Control aviation support Functional task proficiency Handle detainees	Breaching/clearing IEDs Marking/proofing IEDs Reporting/tracking Enhancing IED detection Enhancing surveillance Performing long-range communications Using translators effectively	Urban movement Crowd/riot Antiaircraft attacks Bait/ambush HN security forces Facility/base security "nondoctrinal" conditions Continuous operations Integration of replacements Theater culture	IEDs - to isolate a subunit IEDs - to distract/deceive IEDs - to cause casualties/symbolic target IEDs to protect supplies/workshops/leaders Intimidation of HN security forces IED - with attack on responders Crowds - hostile demonstrations False information from local sources Mortar/rocket attacks on FOBs		
Execute info operations Organize civil and military efforts Collect/process/report information Pattern analysis/targeting Organize shaping efforts Organize sustainment operations Integrate/allocate "nonstandard" capabilities Transition quickly/nonstandard missions Organize/execute replacement operations Apply force discriminately Consequence management	C2 distributed operations Anticipate requirements Clear/concise INTSUMs/FRAGOs Reaction force Reconnaissance Functional task proficiency Contracting management Track detainees	Long-range communications Long-range detection Translators Pattern analysis Aviation support CA support Organic EOD capability Detainee temporary hold capability	Extended distances Distributed capabilities Simultaneous events Continuous operations and sustainment Situational uncertainty HN security forces "nondoctrinal" conditions Integration of replacements SOF operating in AO U.S./non-U.S. media in AO Contractors/local hires	Attacks to identify friendly patterns IEDs - to isolate ambush target IEDs - to bait response forces Antiaircraft attacks Kidnap Soldier or Marine to create media event VBIED against fixed facilities Rocket/mortar attack against fixed facilities Attacks against civilian, ICDC, and NGO targets Local-hire spies inside FOB Attacks against contractors, and local hires		
Plan/direct/coordinate IO campaign Geographic responsibility Coordinate/resource civil/military campaign Allocate resources to subordinates Collect/develop/disseminate intelligence Provide unity of effort/command Control MSRs Conduct consequence management Adapt/modify ROE	Anticipate requirements Disseminate information Adapt procedures quickly Contracting support Interagency coordination Distributed operations Plan/prepare/execute/ sustain/train Proactive decision making Information operations	Political advisors Long-range communications Dedicated security JIM task organization Media/VIP support MWR requirements Dedicated CMOC Movement control	Extended duration and battlespace Concurrent offensive and stability and reconstruction operations Multitask subordinates Simultaneous events Decentralized, unstable condition JIM Integrate new capabilities Constant media information demands Domestic political issues	External military influences Iraqi/tribal political conflicts Media pressure - U.S./non-U.S. CPA priorities International political issues/crises New/changing JIM priorities Enemy tactical adaptation Multiple/diverse/disparate enemies		

Table 8-2. Critical tasks for collective training

Critical/Collective Task	*Supporting Collective Task*	*Supporting Individual Task*	*Leader Task*
Employ the Appropriate FP Measures	19-2-2171 Provide Antiterrorism and Force Protection 03-3-C201 Prepare for Operations Under Chemical, Biological, Radiological, and Nuclear (CBRN) Conditions 05-2-3092 Prepare for a Suspected Vehicle-Borne Implemented Explosive Device (VBIED)/Suicide Bomber Attack		05-1-0035 Control a Base in a Base Cluster 05-6-0068 Conduct Cluster Operations
Establish an Entry Control Point (ECP)	19-4-4900 Establish Access Control Point (ACP) Operations 19-4-4901 Plan Access Control Operations	191-376-5151 Control Access to a Military Installation	191-378-5315 Supervise an Installation Access Control Point 191-379-4430 Develop an Access Control Training Program
Establish a TCP	19-3-1202 Conduct Route Regulation Enforcement; 19-2-2401 Supervise the Establishment of Roadblocks and Checkpoints	191-377-4202 Supervise the Establishment and Operation of a Traffic Control Post (TCP)	19-1-1201 Prepare Traffic Control Plan 19-2-1202 Supervise Route Regulation Enforcement
Conduct ECP Procedures	19-4-4900 Establish Access Control Point (ACP) Operations 19-4-4901 Plan Access Control Operations		191-377-4214 Supervise Emergency Entrance and Exit Procedures 191-379-4435 Inspect an Access Control Point
Conduct TCP Procedures	19-3-1202 Conduct Route Regulation Enforcement 19-2-2401 Supervise the Establishment of Roadblocks and Checkpoints	191-376-4105 Conduct TCP Procedures	19-1-1201 Prepare Traffic Control Plan 19-2-1202 Supervise Route Regulation Enforcement
Search Vehicles, Personnel, and Equipment	19-4-4900 Establish Access Control Point (ACP) Operations 19-4-4901 Plan Access Control Operations	191-376-5115 Search a Person 191-376-5121 Search a Building 191-376-5122 Search a Vehicle for Explosive Devices or Prohibited Items at an Installation ACP	191-378-5308 Supervise Search for an Individual
Operate a QRF	19-3-2201 Conduct Response Force Operations		19-2-2201 Direct Response Force Operations

Table 8-2. Critical tasks for collective training

Critical/Collective Task	*Supporting Collective Task*	*Supporting Individual Task*	*Leader Task*
Plan a Convoy Movement	19-3-2007 Conduct Convoy Security Operations 05-1-1006 Prepare for Ground Emplaced Improvised Explosive Device (IED) Defeat Operations Prior to Movement 55-2-4003 Conduct Convoy Movement		19-2-2004 Supervise Convoy Security 191-379-4407 Plan Convoy Security Operations
React to a Possible IED (No Detonation)	05-2-3091 React to a Possible Ground-Emplaced Improvised Explosive Device (IED)	191-378-5310 Supervise First Response to a Crisis Incident	
React to an IED Attack			191-378-5310 Supervise First Response to a Crisis Incident
Establish a Cordon	19-3-2206 Conduct a Cordon and Search		19-2-2206 Supervise Cordon and Search Operations 191-377-4203 Supervise the Establishment and Operation of a Roadblock/Checkpoint 191-379-4402 Plan Roadblocks and Checkpoints
Establish a Media Control Point	19-1-D618 Interact With the Media in the Area of Operations 19-2-6018 Support Media in the Area of Operations		
Coordinate and Supervise a Recovery Operation	19-3-2012 Support Area Damage Control Operations		19-2-2012 Supervise Area Damage Control Operations

This page is intentionally left blank.

Appendix A

Metric Conversion Chart

This appendix complies with current Army directives, which state that the metric system will be incorporated into all new publications. Table A-1 is a conversion chart.

Table A-1. Metric conversion chart

U.S. Units	***Multiplied By***	***Metric Units***
Feet	0.30480	Meters
Inches	2.54000	Centimeters
Inches	0.02540	Meters
Inches	25.40010	Millimeters
Miles	1.60930	Kilometers
Pounds	453.59000	Grams
Pounds	0.4536	Kilograms
Metric Units	***Multiplied By***	***U.S. Units***
Centimeters	0.39370	Inches
Grams	0.03527	Ounces
Kilograms	2.20460	Pounds
Kilometers	0.62137	Miles
Meters	3.28080	Feet
Meters	39.37000	Inches
Meters	1.09360	Yards
Millimeters	0.03937	Inches

This page is intentionally left blank.

Appendix B

Intelligence

The process of IPB is the same for counterinsurgency operations as for any other type of operation; however, the important considerations are unique. Special Text (ST) 2-01.301 contains useful guidance on IPB considerations for stability and reconstruction operations that bear directly on counterinsurgency. Some considerations specific to the IED fight are discussed below.

SECTION I – INTELLIGENCE PREPARATION OF THE BATTLEFIELD

DEFINE THE BATTLEFIELD ENVIRONMENT

B-1. A thorough knowledge of the roads in the unit AO is a critical step in the IPB to deal with the IED threat. It supports not only analysis of likely attack points, but development of as many alternate routes for friendly use as possible, thus depriving the enemy of easy patterns to plan attacks against.

B-2. The demographics of the AO and area of intelligence responsibility (AOIR), along with the likely learnings of each ethnic, religious, and socioeconomic group towards friendly forces and the insurgents should be understood. This knowledge will support the analysis of likely attack locations, as well as the ability to successfully use nonlethal engagements, such as psychological operations, CA, and shows of force to interdict insurgent capabilities in the AO.

B-3. A thorough knowledge of the culture and history of the AO and AOIR should be gained. This will provide an understanding of both the insurgents and the local population and help prevent handing the enemy costly IO victories.

B-4. The key leaders in the AO and AOIR should be identified as thoroughly as possible and the power structures they use both official and informal (priests, crime bosses, influential and prominent people, or families).

DESCRIBE THE BATTLEFIELD EFFECTS

B-5. Terrain analysis, specifically along the roads in the AO, is an important consideration when conducting IPB with the IED threat in mind. While IED attacks are feasible virtually anywhere and at any time, certain features provide particularly suitable situations. They are—

- Overpasses, for both hanging and hand-thrown IEDs. (It is important to develop convoy TTP for security at overpasses. Often persistent surveillance and even security is necessary at these locations).
- Places that force slowdowns and closer intervals on convoys, such as winding turns, unpaved surfaces, steep or sharp turns, narrow roadways, and choke points.
- Areas of dense civilian traffic that provide determined insurgents with concealed approach possibilities as well as slow-moving targets.
- Culverts and unpaved roadways that provide opportunities to bury large IEDs directly in the path of a convoy.
- Terrain features that provide overwatch positions that can support use of command-detonated IEDs and combined IED and direct-fire ambushes.
- Metal guardrails that provide hiding places for elevated IEDs.

- Regularly spaced objects, such as telephone poles and street lights that allow insurgents to assess convoy speed and, thus, time their IED detonations more accurately. Convoy commanders need to be aware of these areas.
- Areas in which the population is known or inclined to be hostile to friendly forces. The areas are higher IED attack threats since they are less likely to reveal IED attackers operating in their midst.

B-6. It is also important to develop, as quickly as possible, a detailed knowledge of what is normal along the routes in the unit AO. Understanding what the terrain along the routes normally looks like will facilitate change detection via patrols and IMINT collection that can identify possible IED emplacements. Knowing what is normal in terms of human activity patterns along the route provides an indicator of impending attack when changes are noticed by patrols, HUMINT assets, or other collection methods.

DETERMINE THREAT MODELS

B-7. While insurgents or terrorists do not have doctrine that can be templated in the sense that we think of when dealing with regular armies, they do have methods and TTP that can be understood. These change frequently based on success or failure and changes in friendly procedures. The best way to understand these are to communicate with units already operating in the prospective AOs, or at least keep up with reports coming out of those areas. This is also a case when intelligence reach is important. National agencies, such as the DIA, NGIC, and Marine Corps Intelligence Activity (MCIA) will often follow threat activities in likely hot spots even before decisions are made to deploy U.S. forces there. Things to focus on with regard to IEDs include—

- Favored initiation methods.
- The most common indicators of an emplaced IED (wires protruding from dead animals, fresh holes next to roads, junked cars).
- The kinds of materials used in the IEDs (these can vary even in different parts of the same theater) and their likely sources.
- Favored targets (Do the insurgents prefer to target military forces or terrorize the civilian population? Do certain kinds or configurations of convoys seem to invite more attacks? Certain vehicle types invite more IED attacks.).
- How many different types of IEDs are common, and is there some pattern to their use. (This could suggest how many different IED makers are active and roughly where they operate.)

B-8. If enemy methods are sufficiently well known, create tactical-level templates for use in developing friendly counter-IED TTP for convoys, patrols, and so forth. If not, then make the best representative templates possible based on experiences in other AOs and/or previous conflicts (the more recent the better). This is not as bad a solution as it may sound; insurgents and terrorists communicate successful TTP worldwide via the Internet, and often what works in one part of the world will appear quickly in others.

DETERMINE ENEMY COURSES OF ACTION

B-9. IEDs are a tactic of insurgents, so most likely the S-2 or G-2 will incorporate IEDs within larger enemy COAs developed in preparation for wargaming. The nature and use of IEDs that the S-2 will predict depends on the knowledge of the goals, objectives, and technical capabilities of the insurgent force, areas with sympathetic populations and, above all, on past experiences and patterns. For example, an insurgency that is primarily foreign-based or based on a specific ethnic or religious group may be willing to launch attacks that target local populations, while one that is nationalistic or operating among its own people might not. Insurgencies aiming to overthrow a government may focus more on governmental, military, and police structures, while those seeking redress of more specific grievances may focus more tightly on those elements closely associated with those grievances (such as upper-class economic targets). How an insurgency uses IEDs will be part of this larger framework of goals and intent. In terms of IEDs specifically, technical capabilities (current and predicted) are important, while the most important considerations of all are recent methods and trends.

B-10. As with standard IPB, the G-2 or S-2 will develop an event template (Figure B-1) with NAIs and likely enemy actions noted, to include likely IED attack sites based on the complete IPB process up to this point.

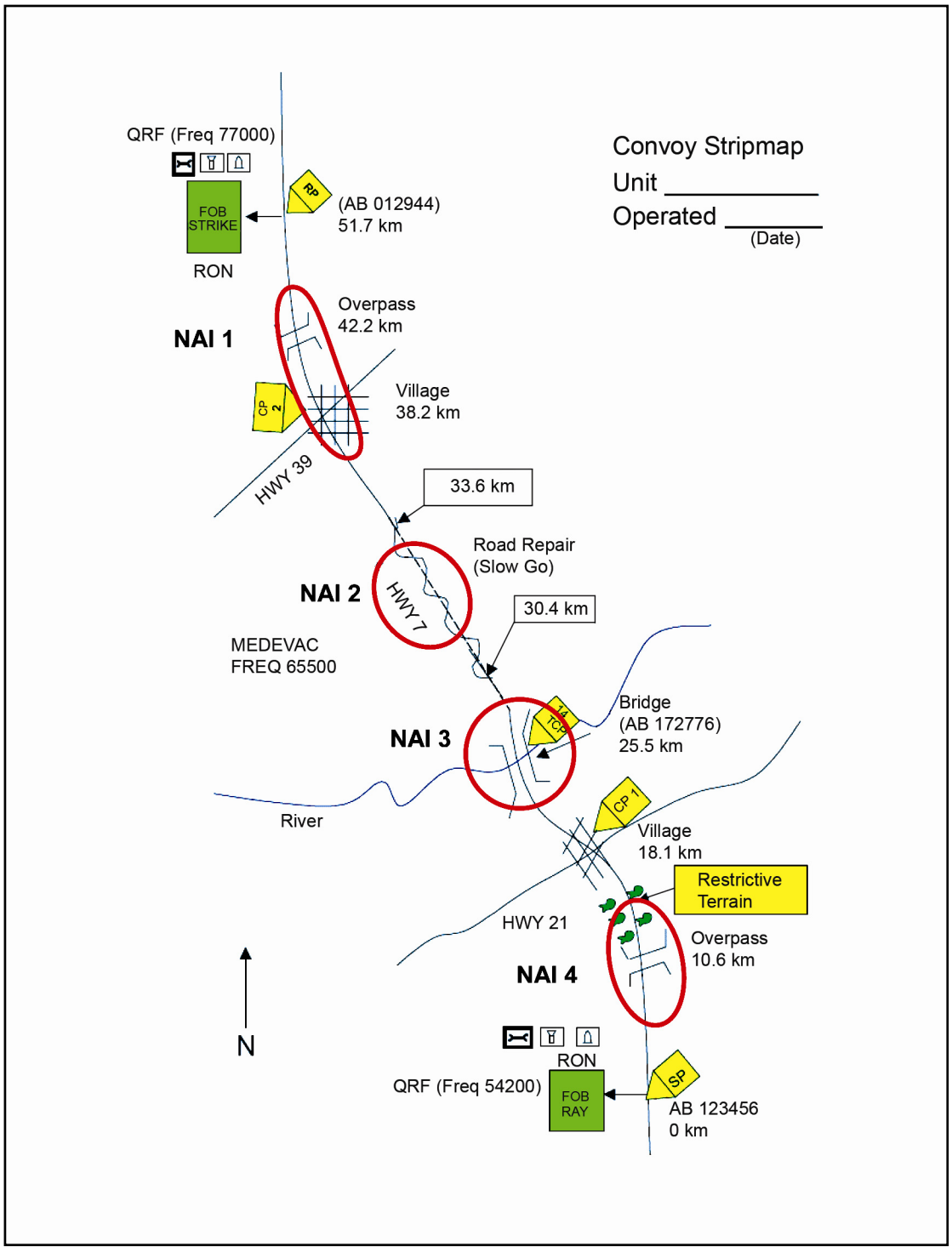

Figure B-1. Event template

B-11. Wargaming specifically for IED attacks is most useful when developing counter-IED TTP for convoys, patrols, and checkpoint and base defenses. In this case, the G-2 or S-2 should begin by building templates based on known recent enemy methods or the best representative methods if the current enemy is not yet well known. Then, the G-2 or S-2 should think creatively and attempt to predict other methods that are within the estimated capabilities of the enemy and most dangerous to friendly forces. These become the basis against which friendly-planners model and fight their prospective TTP. The G-2 or S-2 should update the enemy templates as new methods become apparent in enemy actions and detected planning and training.

SECTION II – COLLECTION ASSETS

B-12. Intelligence collection assets encompass both organizations and systems that gather combat information and intelligence to provide SU and enable the commander to make timely decisions. These assets are categorized in functional terms by intelligence disciplines, such as HUMINT, SIGINT, IMINT, measurement and signature intelligence (MASINT), and TECHINT. The following is a brief description of the assets and organizations within each discipline available to the tactical commander and their uses in the IED fight.

HUMAN INTELLIGENCE

B-13. See FM 2-0 and ST 2-22.7 human intelligence. HUMINT is the collection, by a trained HUMINT collector, of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligence requirements and cross cue other intelligence disciplines. In practical terms, it can range from interviewing a person who walks up to a patrol to volunteer information through use of recruited sources. All Soldiers and Marines can potentially collect HUMINT in some fashion. Specially trained HUMINT personnel (enlisted military occupational specialty [MOS] 97E, warrant 351E, officer 35E) conduct active collection through the use of recruited sources. These Soldiers and Marines are also trained to conduct interrogations of captured enemy personnel and exploitation of documents and media. HUMINT personnel are organized in two- or four-Soldier tactical human intelligence teams (THTs) from EAC down to BCT level and can be task-organized further down at the commander's discretion.

B-14. Time and security are the two critical factors in planning to make use of HUMINT assets. THTs is not a sensor that can simply be emplaced and instantly begin collecting (finding and recruiting reliable sources takes time, and a change in collection targets can often entail the need to recruit new sources). Also, THTs are small and lightly armed (in a combat environment, they require security support in order to function). Methods can include, but are not limited to, being placed in a secure location, such as a unit base or at a civil-military operations center (CMOC), being included in patrols, being included with psychological operations or CA units when they conduct missions, or being sent out to find and meet sources with a dedicated security element.

B-15. Through the use of source operations, local national, local employee, and walk-in screening and debriefings, interrogations, and document exploitation, HUMINT assets can contribute to the IED fight. This includes—

- Identifying hostile personnel in the unit AOs, including IED makers, emplacers, and suppliers.
- Determining connections between known or suspected hostile personnel, and thus building a detailed understanding of enemy organizations and their structure in the unit AO.
- Identifying and locating hostile organizations, meeting places, supply caches, materiel sources, and C2 elements.
- Providing indications and warnings of impending IED activities.
- Revealing enemy perceptions of friendly patterns and vulnerabilities.
- Understanding enemy intentions, objectives, goals, and methods.

B-16. HUMINT provides the ability to detect, identify, and understand an insurgent enemy in sufficient detail to target and defeat it. In a counter-insurgency or stability and reconstruction operation type environment, HUMINT is the primary collection asset.

COUNTERINTELLIGENCE

B-17. See FM 2-0 and ST 2-22.7 for counterintelligence. CI is closely related to the HUMINT discipline in that both rely on the use of recruited sources and other human interaction. Due to the low density of both and their similar skill sets, CI personnel (MOS 97B, 351B, and 35C) are often used interchangeably with HUMINT personnel at the tactical level. These Soldiers and Marines can conduct source operations and interrogations in a manner similar to HUMINT personnel. They do, however, provide some unique capabilities of use in the IED fight.

B-18. The mission of CI is to counter or neutralize hostile intelligence collection efforts through collection, CI investigations, operations, analysis and production, and functional and technical services. CI personnel are trained to understand hostile collection capabilities across all intelligence disciplines in order to be able to advise the commander on countermeasures. They can—

- Detect and train others to detect enemy attempts at intelligence collection and surveillance against the unit.
- Develop countermeasures to neutralize or limit enemy collection capability.
- Screen local national employees in order to detect and prevent potentially hostile personnel from infiltrating the unit by this means.
- Be a liaison with allied and HN organizations (such as military, law enforcement, and intelligence) to provide information to the commander on threats within the AO.

B-19. In higher-level organizations working at corps or EAC, CI personnel also have at their disposal technical capabilities, such as polygraph and technical collection detection. To access these capabilities, tactical units coordinate through their division G-2 to the corps-level C2.

SIGNALS INTELLIGENCE

B-20. See FM 2-0 and ST 2-50 for signals intelligence. SIGINT is the sum total of intelligence derived from the interception and exploitation of foreign electronic signals. It includes communication intelligence (COMINT) (derived from enemy communications signals), electronic intelligence (ELINT) (derived from noncommunications emitters, such as radar), and foreign instrumentation signals intelligence (FISINT) (derived from emissions associated with testing and operations of hostile aerospace, surface, and subsurface systems).

B-21. At the BCT and division level, organic SIGINT assets operate the Prophet, a high-mobility, multipurpose wheeled vehicle (HMMWV)-mounted COMINT collection system. It can collect from stationary positions and on the move. The system can also be dismounted from the vehicle as the PRD-13 manpack version. The system is capable of collection and direction finding against the full range of military-style communications devices and a variety of nonmilitary devices as well. Technical inserts, such as a Prophet, Hammer, and Cobra, can further expand the collection capability. MOS 98G personnel (SIGINT intercept) operate the system themselves and listen to intercepted signals to derive immediate intelligence and combat information, and 98C personnel (SIGINT analysts) within the collection unit and in G-2 sections at division and higher analyze the signals and emitters to derive further intelligence.

B-22. The actual collection range of the Prophet System depends on the radio line of sight, the strength of the transmitter that produces the intercepted signal, and interference from other emitters or weather and atmospheric conditions. While a single Prophet System is capable of direction finding, it requires three or more systems working together on the same signal at the same time to develop a targetable location of the emitter.

B-23. At the corps level, the guardrail common sensor (GRCS) is the organic collection system. This is an airborne collection system mounted in an RC-12 fixed-wing aircraft. It is capable of both COMINT and ELINT collection and direction finding and can provide targetable locations of emitters. With coordination, division intelligence sections can receive the data collection from GRCS in near real time. Units at lower echelons can request intelligence products and data derived from GRCS missions.

B-24. Division and corps sections also have access to joint and national SIGINT data via the Division Tactical Exploitation System (DTES) and the Tactical Exploitation System (TES). These systems provide detection and locations of emitters as well as imagery download and exploitation capability. When dealing with the IED fight, tactical SIGINT can—

- Determine hostile plans, intent, and objectives.
- Give indications and warnings of impending enemy activities including IED attacks.
- Identify hostile personnel and links between such persons and organizations.
- Provide indications of popular sentiment and reactions to specific friendly and enemy actions.
- Identify and provide at least general locations of emitters associated with IED attacks in order to cue other collection assets, such as HUMINT.

B-25. In a counterinsurgency environment, SIGINT is not as prolific of a collection discipline as HUMINT. The unstructured nature of nonmilitary and insurgent communications and the lack of signature devices, as well as the urban environment common in such fights, make SIGINT collection less immediately targetable than in a major combat operation. However, it does have some advantages. In terms of content, since the subject is not aware of being listened to, it can be a better indicator of true feelings and intent than even a reliable HUMINT source who is aware of the impact of the words of the subject on the collector. It also provides 24/7 operation capability. Finally, once identified, known enemy emitters can be readily monitored every time they activate, and the information provided to analysts is in near real time.

IMAGERY INTELLIGENCE

B-26. See FM 2-0 and ST 2-50 for imagery intelligence. IMINT is derived from the exploitation of imagery collected by visual photography, infrared, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, digitally on film, electronically on display devices or other media. There are a variety of imagery systems whose use or capability is available to the commander in the IED fight. These systems include—

- **Ground surveillance radar.** Ground surveillance radar (GSR) sections currently exist within the MI company of the BCT. In these sections, 96R Soldiers operate the PPS-5 (in heavy units) or PPS-15 (in light units) GSRs. These systems are capable of providing persistent surveillance over an area of several square kilometers, through darkness, fog, and smoke, detecting and locating personnel or vehicles moving in the search area. In the IED fight, these systems can be used to detect enemy personnel emplacing IEDs.
- **Unmanned aerial vehicles.** UAVs provide optical and infrared imagery in real time to ground stations and, in some cases, over other broadcast systems. UAVs allow the commander to actually see beyond the line of sight of his own units. The advantage of UAVs is that they provide data in a form very similar to what a Soldier or Marine would see with his own eyes, without risking a Soldier or Marine to do so, over extended distances. The main limitations of UAVs are the weather, airspace control, the range and endurance of the system, and the limited area the system observes at any given time. Systems available in the IED fight include the—
  - **Raven.** A Raven is a small UAV operated at the battalion level, with a flight duration of about 60 minutes and a range of 12 kilometers. It provides electro-optical (daytime) and infrared (nighttime) video imagery directly to a ground control terminal and one remote terminal per system.
  - **Shadow.** A Shadow platoon is organic to each BCT. The system itself has a rated range of 75 kilometers, an endurance of 4 hours, and has electro-optical and infrared sensors on board. It provides imagery directly to one or more ground control stations, which can in

turn, broadcast video via local area network (LAN) or other digital communications devices.

- **Hunter.** The Hunter is operated at the corps level. It has a range of 200 kilometers, an endurance of 10 hours, and carries an electro-optical and infrared payload. It provides imagery directly to one or more ground control stations, which can in turn, broadcast video via LAN or other digital communications devices, as well as to remote video terminals, the Air Force remote operations video-enhanced receiver (ROVER) terminal, and the Global Broadcast System (GBS) satellite network.
- **Predator.** The Predator is an Air Force long-range unmanned UAV that can provide support to ground forces on a request basis. It has a range in excess of 300 kilometers and an endurance of 40 hours. It carries electro-optical and infrared payloads and can also carry Hellfire missiles and a laser designator for a targeted attack. It provides imagery directly to one or more ground control stations, which can in turn, broadcast video via LAN or other digital communications devices, as well as to remote video terminals, the Air Force ROVER terminal, and the GBS satellite network.

- **Joint Surveillance Target Attack Radar System.** The Joint Surveillance Target Attack Radar System (J/STARS) is an Air Force collection platform that provides moving target indicator (MTI) detection over a wide area of the battlefield. The system can detect moving vehicles and to some extent differentiate between tracked and wheeled vehicles in real time. It broadcasts data to the common ground station (CGS) which is present in Army units down to the BCT. In the counterinsurgency and IED fight, it can provide the following:
  - Time-phased depictions of vehicle traffic patterns in the unit AO that shows routes that locals use and those they avoid.
  - Detection of vehicle movement through specific NAIs that may indicate insurgent movements.
  - Detection of a high volume of traffic in unpopulated areas that could indicate meeting or training areas.
  - Track the movement of vehicles into and out of the location of an IED attack that could indicate the movement of IED emplacers or reconnaissance elements and track them back to the point of origin.
- **Tactical Exploitation of National Capabilities.** Tactical exploitation of national capabilities (TENCAP) systems, such as the mobile integrated tactical terminal (MITT) and DTES, present at the division G-2 allows for near-real-time download and exploitation of national-level imagery collection. In terms of the IED and counterinsurgency fight, such imagery can be used for long-term change detection, periodic surveillance of suspected insurgent safe houses or training areas, and updating known terrain and map data.
- **Buckeye.** The Buckeye consists of a remote sensing capability which collects high-resolution color photography for change detection and identification of IED sites. Color imagery is collected and processed after flying a selected route, at which time the images are geo-referenced with coordinates which enable image analysts to identify potential IEDs. The Buckeye capability is deployed to selected brigade units in-theater and is supported by field teams from the United States Army Topographic Engineering Center, Alexandria, Virginia.

B-27. Imagery systems provide the commander with a visual depiction of enemy activity in the battlespace. The advantage is that it can often make clearly apparent what is difficult to grasp in data from other sensors. Also, many imagery systems can collect without alerting the insurgents to the collection effort. Imagery systems (in particular airborne and space-based platforms) are limited by weather and are vulnerable to deception via the use of camouflage and mock-ups. Infrared and radar imagery in particular requires interpretation by trained IMINT personnel (MOS 96D and 352G).

MEASUREMENT AND SIGNATURE INTELLIGENCE

B-28. See FM 2-0 and the Remotely Monitored Battlefield Surveillance System (REMBASS)/Improved-REMBASS System Training Plan for measurement and signature intelligence. MASINT is technically

derived intelligence that detects, locates, tracks, identifies, and/or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from the IMINT and SIGINT collection. MASINT collection systems include, but are not limited to, radar, spectroradiometric, electro-optic, acoustic, radar frequency, nuclear detection, and seismic sensors, as well as techniques for gathering nuclear, biological, and chemical (NBC) and other material samples.

B-29. Within tactical units, the MASINT system is the REMBASS. The REMBASS is a ground-based, all-weather, day-and-night, battlefield surveillance, target development, and early warning system capable of remote operation under field conditions. The system consists of eleven major components: a passive infrared sensor, magnetic (MAG) sensor, a seismic/acoustic sensor, a radio repeater, a sensor monitoring set (SMS), a radio frequency monitor (referred to as portable monitoring set [PMS]), a code programmer, an antenna group, a power supply, a mounting rack, and a sensor signal simulator (SSS). A set consists of 8 IR sensors, eight MAG sensors, 32 seismic/acoustic sensors, 8 radio repeaters, one SMS, 3 PMS, 2 code programmers, 1 antenna group, 1 power supply, 1 mounting rack, and 1 SSS. Enlisted personnel (96R or 98P) operate the system and can train others in its operation. REMBASS is organic to the MI companies of infantry, air assault, and airborne BCTs.

B-30. The advantage of the REMBASS is the capability to conduct long-term surveillance of a given piece of terrain without having to commit personnel to the mission. With proper positioning of the sensors, users can detect and identify movement of armed or unarmed personnel, wheeled or tracked vehicles, to include the speed and direction of movement and the number of personnel or vehicles. The sensors are small and can be camouflaged to avoid detection. The disadvantage of the system is the need to manually emplace and recover the sensors and replace batteries in the sensors and relays. In the IED fight, the REMBASS—

- Provides persistent surveillance of frequent IED attack locations to support the capture or kill of IED emplacers.
- Monitors infiltration routes to detect movement of insurgent personnel and supplies.
- Provides persistent surveillance of likely insurgent reconnaissance and/or overwatch positions.
- Detects attempts by insurgents to return to known or suspected weapons or supply caches.
- Monitors the rate and type of dismounted or mounted traffic along a given route or through a given area 24/7.

TECHNICAL INTELLIGENCE

B-31. See FM 2-0 for technical intelligence. TECHINT is derived from the collection and analysis of enemy and other foreign military equipment and associated materiel. The purpose is to determine the level of enemy technological capability and to detect changes or improvements in that capability, in order to predict future enemy abilities in time to develop countermeasures. TECHINT capabilities do not exist within Army tactical units; however, several elements exist in operational theaters that provide support. Specific to the IED fight are the CEXC manned by joint service and coalition EOD personnel, the counter-IED targeting program, WITs, and FBI explosives experts. In the IED fight, these elements can provide the following:

- Databases that track different types of IEDs and can link an IED to a known or suspected maker based on materials and methods used in its construction.
- Analysis of found or captured materials to determine if they are in fact IED precursors.
- Analysis of current IED construction and initiation methods.
- Prediction of IED trends and likely future construction and initiation methods.
- Assessment of possible sources of IED materials based on forensic analysis of IEDs found either before or after detonation.

SECTION III – PROCESS CONSIDERATIONS

B-32. Use of intelligence surveillance (INTS) of various intelligence disciplines (HUMINT, IMINT, SIGINT, and so forth), will be the most important in a counterinsurgency operation. It will provide the most knowledge of enemy personalities, organizations locations, and intentions.

Note. There may be more than one insurgent group operating in your AO, possibly with little or no connection to each other.

B-33. If you have control of HUMINT assets, you will need to organize a control structure, including an operational management team (OMT) at BCT level or a human intelligence operations center (HOC) at division level; an S-2 or G-2 to coordinate with higher, adjacent, interagency, and HN intelligence capabilities; and resource funding, equipment, and rewards to support source operations. ST 2-22.7 provides detailed guidance on the use and conduct of HUMINT.

B-34. In addition to planning how to use the intelligence means at your disposal, organize the analytical assets to take advantage of HUMINT in particular. Functions, such as document exploitation, open source media monitoring, and technical exploitation of items (such as computers, wireless, and cellular telephones) and will be important to the analytical effort. Analysts need to understand such things as link analysis and tools (for example, the analyst notebook); how insurgent forces are organized and operate; the critical needs of an insurgency, to include funding, arms suppliers, safe houses or areas, training areas, and intelligence collection; and insurgent use of IO. Commanders and analysts should be prepared to build and update a situation template based on HUMINT and supplement it by other disciplines.

B-35. Intelligence support to targeting will be much different than what was learned in the schoolhouse. Instead of using the detecting, tracking, and engaging systems, you will be using D3A with the outcome of identifying, locating, and detaining persons and controlling key areas. The main targeting problems will be understanding the insurgent organizations being fought, especially identifying the key people, and then making sure that there is enough accurate information to make attempting to capture the persons worthwhile. It demands a great deal more patience and persistence than targeting in a major combat operation. Use the targeting functions of D3A.

B-36. The ability to establish or link into other intelligence sources is called intelligence reach or accessing of the resources of national, joint, foreign, and other military organizations and these units will be important to you no matter what your echelon. Reporting, databases, feeds from higher HQ and staffs, adjacent, JIM collection systems help complete your picture, and in some cases will determine whether or not your unit executes an operation. Coordinate with your higher intelligence staff and your command, control, communications and computer operations (C4 Ops) officer (S-6) or Assistant Chief of Staff, Command, Control, Communications, and Computer Operations (C4 Ops) (G-6) should be coordinated with to determine what can be accessed and how to get it done.

B-37. Linguists, in particular contract linguists, will be a major concern. They are critical to your ability to conduct HUMINT and CI, perform SIGINT collection, develop psychological operation products, and perform CA and liaison with local national forces and government and NGO elements. Military linguists (primarily 97E in HUMINT and 98G in SIGINT) are proficient enough to perform their duties in a major combat operation; however, being effective in stability and reconstruction operations and counterinsurgency operating environments requires native-level fluency, preferably in the specific dialect common in the AO. Hiring contract linguists with security clearances is generally done through a centralized DOD-level contractor; acquiring, distributing, and managing these linguists is an S-2/G-2 responsibility. The following considerations should be kept in mind:

- Since these linguists are civilians, the theater commander may not allow them to be armed. There will be specific rules governing what they can or cannot do, a combination of the rules governing contractors on the battlefield and specific restrictions applied by the contractor providing the linguists.

- Linguists will often be immigrant U.S. citizens originally from the country or even from the local area in which the unit operates, in which case they will have valuable background knowledge of the AO, as well as biases which must be kept in mind. Additionally, those with local backgrounds may have relatives or friends they want to spend time with, which can place them at significant risk in a counterinsurgency environment.
- Linguists will often be significantly older than the Soldiers and Marines, and in any case much less physically fit, which needs to be considered when planning their use.
- There will never be enough linguists, particularly those with security clearance (meaning U.S. citizens). Carefully plan, before deploying, the priorities for both locally hired and U.S.-contracted linguists; this is a matter for coordination between the S-2, the operations staff officer (S-3), and the civil-military operations officer (S-5) (for the local hires), with approval by the commander. During operations, always maintain a plan to handle sudden reductions in available linguists. Any number of factors can lead to such reductions, and it is good to be prepared.

Appendix C

Organization Contact Information and New Related Force Structure

Organization contact and new force structure information relating to IED defeat operations are provided to assist leaders with a point of departure for gathering the most current and up-to-date assistance and information possible.

SECTION I – ORGANIZATION CONTACT INFORMATION

C-1. This contact information is for organizations in support of IED defeat operations. This is not an all inclusive list of organizations involved in IED defeat, but provides a starting point for essential contacts to request information and training material.

COMBINED EXPLOSIVES EXPLOITATION CELL

<http://www.iraq.centcom.smil.mil/www/new_cexc/cexc_new_one.htm>

COUNTER EXPLOSIVE HAZARDS CENTER

Counter Explosive Hazards Center
ATTN: ATSE-TSM-CM
320 MANSCEN Loop, Suite 115
Fort Leonard Wood, Missouri 65473

Commercial: (573) 563-8165
Defense Switched Network (DSN): 676-8165
Facsimile (Fax): (573) 563-8180
<atsetc@wood.army.mil>
<http://www.wood.army.mil/cehc/>
<www.portal.inscom.army.smil.mil/cehc>

JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT TASK FORCE

Joint Improvised Explosive Device Defeat Task Force
Commercial: (703) 692-6953
DSN: 222-6953
Fax: (703) 697-7135
<http://www.portal.inscom.army.smil.mil/jieddtf>

NATIONAL GROUND INTELLIGENCE CENTER

Commander
National Ground Intelligence Center
2055 Boulders Road
Charlottesville, Virginia 22911-8318
Commercial: (434) 980-7535
DSN: 934-7535
Fax: (434) 980-7823
<http://avenue.org/ngic/>
<http://ngicwss.ngic.army.smil.mil>

NAVAL EXPLOSIVE ORDNANCE DISPOSAL TECHNOLOGY DIVISON

Commanding Officer
Naval Explosive Ordnance Disposal Technology Division
2008 Stump Neck Road
Indian Head, Maryland 20640

Commercial: (301) 744-6800
DSN: 354-6800
<http://naveodtechdiv.jeodnet.mil/default.asp>

RAPID EQUIPPING FORCE

Rapid Equipping Force
10236 Burbeck Road
Fort Belvoir, Virginia 22060-5852

Commercial: (703) 704-0059
Fax: (703) 704-1868
<http://www.ref.army.mil>
Soldiers and Marines, for REF equipment concerns, contact: <ref.logistics@belvoir.army.mil>
Commanders, contact REF HQ at <ref.operations@belvoir.army.mil>

TECHNICAL SUPPORT WORKING GROUP

<http://www.tswg.gov>

Explosives Detection
<http://www.tswg.gov/tswg/ed/ed_ma.htm>

Improvised Device Defeat
<iddsubgroup@tswg.gov>
<http://www.tswg.gov/tswg/home/home.htm>

UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND

<http://www.inscom.army.mil>
<http://www.portal.inscom.army.smil.mil>

UNITED STATES ARMY TOPOGRAPHIC ENGINEERING CENTER

United States Army Corps of Engineers®
Engineer Research and Development Center (ERDC)
Topographic Engineering Center
7701 Telegraph Road
Alexandria, Virginia 22315-3864

Commercial: (703) 428-6600
<http://www.tec.army.mil>
<https://www.tec.army.smil.mil>

UNITED STATES MARINE CORPS WARFIGHTING LABORATORY

United States Marine Corps Warfighting Laboratory
IED Working Group
3255 Meyers Avenue
Quantico, Virginia 22134

Commercial: (703) 432-0457
<http://www.mcwl.quantico.usmc.mil/>

UNITED STATES AIR FORCE FORCE PROTECTION BATTLELAB

United States Air Force Force Protection Battlelab
1517 Billy Mitchell Boulevard
Lackland Air Force Base, Texas 78236-0119

Commercial: (210) 925-1497
DSN: 945-1497
<http://wwwmil.lackland.af.mil/Battlelab/index.asp>

SECTION II – NEW RELATED FORCE STRUCTURE

C-2. The force structures discussed below are of the new organizations related to IED defeat operations. This is not an attempt to provide an all-inclusive presentation of organizational structures, but to present recent changes.

CLEARANCE COMPANY

C-3. The paragraphs below describe a clearance company (Army only).

MISSION

C-4. The clearance company conducts detection and neutralization of explosive hazards along routes and within areas in support of support brigades to enable force application, focused logistics, and protection.

CAPABILITY

C-5. The clearance company capabilities—

- Provide training readiness and oversight of assigned route and area clearance platoons.

- Provide battle command for 3 to 5 route, area, or Sapper platoons operating as an engineer team in the execution of route or area clearance missions.
- Clear a total of 255 kilometers of two-way route per day (3 routes of 83.67 kilometers each).
- Clear a total of 2 acres (8,093 meters^2) per day (2 areas at 1 acre each).

Figure C-1 shows the unit symbology and the base table of organization and equipment (TOE) for the clearance company.

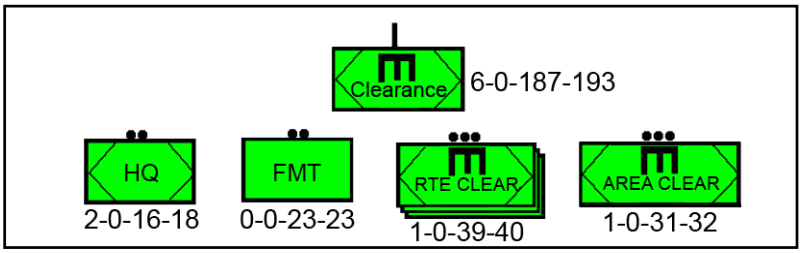

Figure C-1. Clearance company

SUPPORT REQUIREMENTS

C-6. The clearance company supports maneuver or support brigades or JIM forces with explosive hazard detection and neutralization capability as part of an engineer team/engineer mission force (EMF) enabling force application, focused logistics, or protection. The clearance company is dependent upon—

- The SES dog team and the EHT.
- The mine dog team and Sapper platoon.
- The lift capability to load and unload mine rollers.
- The reach-back capability to technical expertise.

EXPLOSIVE HAZARDS COORDINATION CELL/EXPLOSIVE HAZARDS TEAM

C-7. The paragraphs below describe the EHCC/EHT.

MISSION

C-8. The EHCC/EHT gathers and tracks explosive hazards incidents and provides pattern analysis of explosive hazard incidents.

CAPABILITY

C-9. The EHCC/EHT provides explosive hazard SU in-theater/JOA and provides prediction of mobility impediments. Figure C-2 shows the unit symbology and the base TOE for the EHCC/EHT

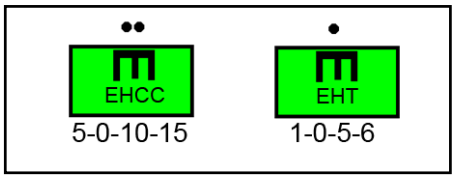

Figure C-2. Explosive hazards team

SUPPORT REQUIREMENTS

C-10. The EHCC/EHT supports corps and division HQ, ME brigades, or engineer brigades with collection, analysis, and dissemination of explosive hazard information. The EHCC/EHT is dependent upon—

- The topographic analysis unit.
- The reach back capability to technical expertise at CBRNE defense cells.
- The criminal investigator for forensics investigation provided by the military police or criminal investigation division organization responsible for area coverage.

MOBILITY AUGMENTATION COMPANY

C-11. The paragraphs below describe the MAC.

MISSION

C-12. The mission of the MAC is to—

- Conduct assault gap crossings and mounted and dismounted breaches.
- Emplace obstacles in support of maneuver BCTs and support brigades to enable force application, focused logistics, and protection.

CAPABILITY

C-13. The MAC—

- Provides training readiness and oversight of assigned assault and obstacle platoons.
- Provides battle command for three to five assault, obstacle, or Sapper platoons operating as an engineer team in the execution of mobility and countermobility missions.
- Enables a maneuver BCT to conduct four assault gap crossings.
- Enables an infantry or Stryker BCT to conduct four mounted breaches.
- Enables a heavy BCT to conduct two mounted breaches.
- Enables a maneuver BCT to conduct four additional dismounted breaches.
- Emplaces 4,432 linear meters of fix/disrupt tactical obstacle frontage without reload.
- Employs two breach platoons to execute hasty route clearance operations.

Figure C-3 shows the unit symbology and the base TOE for the MAC.

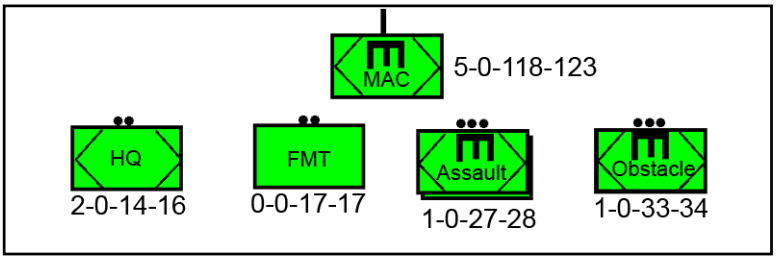

Figure C-3. MAC

SUPPORT REQUIREMENTS

C-14. The MAC supports maneuver or support brigades with gap crossing, assault breaching and countermobility capability enabling force application and protection. They are capable of having a command and support relationship to the maneuver BCT, JIM forces, or as part of an engineer team/EMF. The MAC is dependent upon the maneuver BCT Sapper company.

SAPPER COMPANY

C-15. The paragraphs below describe the Sapper company.

MISSION

C-16. The mission of the Sapper company is to—

- Execute mobility, countermobility, and survivability tasks.
- Provide support of general engineering missions in support of maneuver and support brigades to enable force application, focused logistics, and protection.
- Reinforce engineers in maneuver BCTs.

CAPABILITY

C-17. The Sapper company capabilities—

- Provide training readiness and oversight of assigned Sapper platoons.
- Provide battle command for three to five Sapper, assault, obstacle, clearance, or tactical bridge platoons operating as an engineer team in the execution of mobility, countermobility, and survivability missions.
- Execute 120 kilometers of hasty route clearance per day.
- Execute six dismounted or urban breach lanes.
- Execute three mounted breach lanes.
- Improve lanes and marking in the BCT rear area.
- Employ engineer units to emplace LOC bridges.
- Receive and analyze GSTAMIDS/ASTAMIDS data from other units.
- Provide 660 man-hours per day for general construction labor tasks to vertical, horizontal, or BCT companies during general engineering missions (10 hours per day for sergeant [E-5] and below).

Figure C-4 shows the unit symbology and the base TOE of the Sapper company.

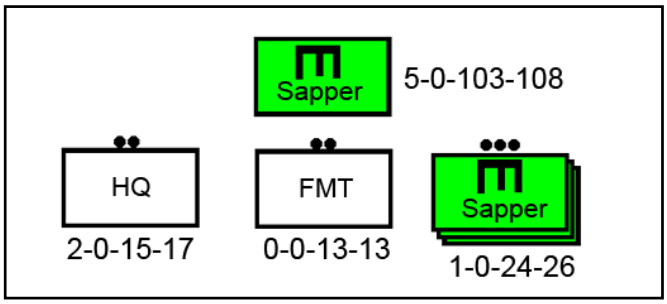

Figure C-4. Sapper company

SUPPORT REQUIREMENTS

C-18. The Sapper company supports the maneuver or support brigades with hasty route clearance, dismounted breach, limited countermobility, and general construction manpower capability enabling force application and focused logistics. They are capable of a command and support relationship with the maneuver BCT, JIM forces, or as part of an engineer team/EMF. When augmented, they can support maneuver or support brigades with deliberate route clearance, mounted breaching, gap crossing, countermobility, and general engineering capability enabling force application, focused logistics, and protection.

C-19. The Sapper company is dependent upon the maneuver BCT, breach squad, route clearance platoon, vertical platoon, and the rapidly deployable earthmoving (light) (RDE-L) or rapidly deployable earthmoving (medium) (RDE-M) platoon.

Appendix D

Recording and Tracking Improvised Explosive Devices

Obtaining and disseminating accurate information regularly is the key to battlefield management and superior SU. Reporting and recording IED field information is critical to the success of the mission and the overall SU of a unit and its leadership. Proper recording and tracking of IEDs not only provides actionable and tactical data for the commander, but it also provides FP information to subordinate and adjacent units through establishment of a COP and allowing such tasks as pattern analysis to be conducted. Pattern analysis is the ability to observe a selection of events or actions over a period of time in a defined location or area. It is used to discover likely patterns or similarities that lead to a logical conclusion that the action or event will occur again in the same location. For instance, over a period of weeks or months a unit encounters IEDs along the same 1-kilometer stretch of route in different locations, but basically with the same design or makeup. Even though these IEDs (once detonated or disarmed) do not populate the COP, their locations plotted over time begin to show a pattern that can be analyzed and used to possibly prevent further occurrences by killing or capturing the unit, person, or persons responsible for emplacing the IEDs. The ability to report and track IEDs throughout the AO is critical to mission success.

REPORTING

D-1. When a unit encounters a suspected IED and leadership confirms it, they immediately report per the unit SOP using the 9-line explosive hazard spot report format. Units must provide timely, adequate information to their higher HQ to ensure that follow-on elements are well informed. Information must include known or suspected IED locations, types of IED (if known), the time encountered, and any additional information that may be of use to the EOD response personnel. The 9-line explosive hazard spot report is the first step in the process and allows for immediate action and decisions to occur.

EXPLOSIVE HAZARD SPOT REPORT

D-2. The explosive hazard spot report is the critical report sent when units encounter an IED while on patrol, in convoys, and so forth. The explosive hazard spot report format can be found in FM 21-16/MCWP 3-17.3. Graphic Training Aids (GTAs) 09-12-001 and GTA 90-01-001 also contain the report format, and leaders should ensure that all Soldiers and Marines have a copy. The report should be submitted as soon as possible (local SOPs will indicate the time requirements). The explosive hazard spot report contains the following nine lines:

- **Line 1, Date-Time Group.** Provide the date-time group (DTG) that the item was discovered (for example, 181230ZMAY05).
- **Line 2, Reporting Unit and Location.** Provide the unit identification code (UIC) of the reporting activity unit and the location of the explosive hazard in an 8-digit grid coordinate.
- **Line 3, Contact Method.** Provide the radio frequency, the call sign, the point of contact, and the telephone number.
- **Line 4, Type of Munition.** Note the size, the quantity, the type of ordnance (dropped, projected, placed, possible IED, or thrown), and the subgroup, if available. If antihandling devices were used, indicate the emplacement method and type of initiation device.

- **Line 5, Chemical, Biological, Radiological, and Nuclear Contamination.** Be as specific as possible.
- **Line 6, Resources Threatened.** Report any equipment, facilities, or other assets that are threatened.
- **Line 7, Impact on Mission.** Provide a short description of the current tactical situation and how the presence of the explosive hazard affects the status (for example, delayed, diverted, cancelled).
- **Line 8, Protective Measures Taken.** Describe any measures taken to protect personnel and equipment (for example, marked).
- **Line 9, Recommended Priority (Immediate, Indirect, Minor, No Threat).** Recommend a priority for response by EOD technicians. Ensure that the priority requested corresponds with the tactical situation you described on line 7 of the report (Impact on Mission). These priorities refer only to the explosive hazards impact on the current mission. A priority of MINOR or NO THREAT does not mean that the explosive hazard is not dangerous.
  - **Immediate.** Stops the maneuver and mission capability of the unit or threatens critical assets vital to the mission.
  - **Indirect.** Slows the maneuver and mission capability of the unit or threatens critical assets important to the mission.
  - **Minor.** Reduces the maneuver and mission capability of the unit or threatens noncritical assets of value.
  - **No Threat.** Has little or no affect on the capabilities or assets of the unit.

DISPOSITION REPORT

D-3. As EOD units neutralize IEDs, they report the disposition according to EOD procedures. See Standardization Agreement (STANAG) 2430 and STANAG 2221.

RECORDING

D-4. Currently there is no standardized methodology for recording and tracking explosive hazards. An explosive hazard numbering system that complements the normal obstacle numbering system can be found in FM 90-7. Once discovered, all explosive hazards have the same impact for reporting requirements and must be accounted for and eventually cleared.

D-5. The explosive hazard numbering system has two primary purposes. These purposes are—

- To give units a method of recording, organizing, and tracking the discovered explosive hazard.
- To provide a record of the discovered explosive hazard to follow-on units or organizations for awareness or possible clearance.

D-6. The explosive hazard number is designated by the HQ that enters the discovered IED information into the database. Once an explosive hazard is entered into a tracking database, it is permanent. After it has been cleared (detonated, removed, or rendered safe), the tracking status will change, but the item remains in the database for future use.

TRACKING

D-7. The MEOICC is the central repository at the tactical operational level that tracks all explosive hazards in-theater. The EHCC will replace the MEOICC in the future.

D-8. The CEXC collects information on IED incidents and prepares, publishes, and disseminates throughout theater, a comprehensive report for every IED incident.

Note. An IED incident includes any unplanned activity involving an IED. It also includes near misses that could have resulted in potential damage or injury.

D-9. Division and maneuver brigade engineer planning cells must establish a central control cell for IED clearance information. The central control cell—

- Maintains a current situation map and an overlay that depicts IED activity.
- Maintains and updates information on IED tracking and route status.
- Maintains a database of IED information and forwards information according to the SOP.
- Processes, analyzes, updates, and disseminates the information to subordinate commanders and staff.

D-10. Other services and organizations execute specific procedures to collect, record, track, and report explosive hazards information. The standardization of tracking this information is critical to the planning and execution of missions in an IED environment.

EXPLOSIVE HAZARDS DATABASE

D-11. The MEOICC uses the Maneuver Control System (MCS) EHDB to manage explosive hazard information. The EHDB is a geo-referenced database system that takes advantage of true geographic information systems (GIS) functionality. The EHDB provides a capability to input, manage, track, and disseminate explosive hazard data to maneuver units and to conduct pattern analysis on the use and location of potential IED sites.

Note. Other services execute specific procedures to collect, record, track, and report explosive hazard information. The centralized management of this information is critical to the planning and execution of missions in an IED environment.

D-12. The EHDB is also used to—

- Provide a capability to manage all hazard information for Army and joint operations.
- Provide a comprehensive hazard tracking capability for all minefields, IEDs, UXO, and enemy ammunition caches in-theater.
- Provide tools that assist in developing strategies for IED activity.
- Support predeployment IPB for theater with hazard intelligence and assist in the MDMP.
- Communicate with higher HQ to maintain up-to-date information.
- Provide data interoperability with command and control personal computer (C2PC), MCS-light, and Falcon View.
- Provide a means to collect and disseminate hazard data at any echelon. Outputs include raw data for trend analysis, TDA, and mobility/map decision aids (MDA) in the form of maps, overlays, and graphics.
- Conduct analysis on the explosive hazard data within the theater to support assured mobility to dominate land operations.
- Use the standard report format. See FM 90-7 for further details.

D-13. The EHDB team is responsible for the input, analysis, product production, and management of the EHDB. EHDBs are also used by organizations other than the MEOICC to track explosive hazard data.

D-14. The Global Minefield Database (GMFDB) is maintained at the United States. Army Engineer School by the CEHC. The GMFDB collects information from the various EHDBs, merges the data into one database, and sends the updated information back to the field.

JOINT DIGITAL INCIDENT GATHERING SYSTEM

D-15. The Joint Digital Incident Gathering System (JDIGS) database compiles EOD incident and technical reports primarily for EOD and countermeasures development organizations. The JDIGS is a searchable database that allows access to these finished reports based on user queries. JDIGS database does not produce machine-readable, formatted data for export or use in geospatial representations for use by maneuver commanders.

FUTURE DATABASE

D-16. The Army is working towards a future, joint digital integrated explosive hazard database that merges current Army Battle Command System (ABCS) into a single system. The MEOICC/EHCC is a likely choice for the repository of this single system.

D-17. Information would be reportable via Force XXI battle command-brigade and below (FBCB2)/MCS-light/ABCS systems. The reporting unit would populate the database directly, as opposed to "through" a specific command post (CP).

D-18. The database would link into COP graphics simultaneously and be displayed in unit tactical operations centers (TOCs) on an explosive hazard overlay. The data could include minefield information, UXO locations, IED trend patterns, and so forth, and units could filter and tailor the information as deemed fit. The information could be used by CPs for various functions—predict explosive hazard information by S-2s and engineers; coordinate detection assets; plan and coordinate EOD and engineer neutralization and disposal capabilities; divert units to different routes to avoid hazards; prevent enemy emplacement of explosive hazards through planned and coordinated combat patrols; and protect forces using the technical information in the database to synchronize CREW systems.

D-19. The database would be extensive and expand beyond the current capabilities of the EHDB. As EOD and engineer units dispose of explosive hazards, they would report the disposals using the same systems, and COP graphics would be automatically populated with the correct information displaying the removal of the explosive hazards from routes and areas. The database will be able to communicate automatically with the JDIGS. Future databases may include JDIGS capabilities in order to migrate to a single explosive hazard system that is useful for all organizations. See Figure D-1.

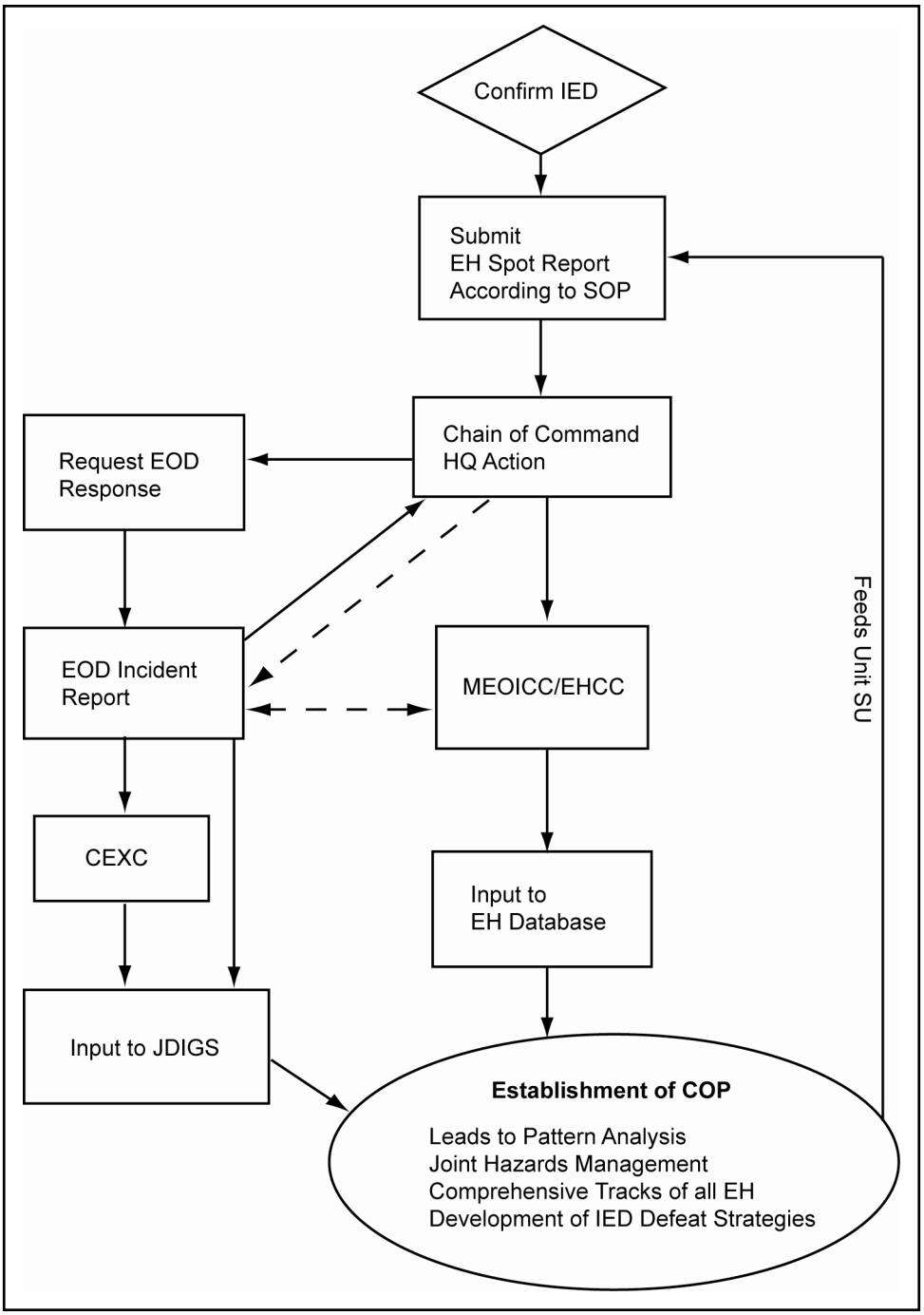

Figure D-1. Explosive hazard spot report flow

This page is intentionally left blank.

Appendix E

Tactics, Techniques, and Procedures Considerations

This appendix provides emerging considerations in TTP and drills in support of planning considerations for IED defeat. It provides immediate action drills and risk mitigation and describes the mobility corridor LOC security.

IMMEDIATE ACTION DRILLS

E-1. To plan immediate action drills, gather existing battle drills and refine them. Immediate action drills are based on the following activities:

- Executing a counterambush drill and immediately focus outward. (The biggest mistake our troops make is focusing inward towards the site of the IED. Obviously, some will have to focus inward. The unit needs to develop a battle drill to identify who pulls security and who focuses inward. It cannot be by name, because the unit does not have the choice of who will be hit by the IED.)
- Moving out of the kill zone (depending on the unit TTP). Seeking cover and concealment if stopped.
- Being prepared to maneuver against the enemy.
- Capturing or killing anyone in the general area of a command-detonated IED.
- Ensuring that Soldiers and Marines know and understand the ROE.
- Reporting contact with an IED using the explosive hazard spot report.
- Establishing and maintaining 360° security. Watching for enemy and enemy-associated activities (personnel fleeing with or without weapons, vehicles rapidly departing the area, personnel with LRCTs, video recorders or some type of remote device, small arms fire, drive by shootings, and so forth). Searching (in detail) for personnel that may command detonate the IED; this is paramount in order to support bomb maker targeting. Capturing these personnel is a priority, killing only when necessary and detaining all other suspect personnel.
- Searching the immediate safe area. Using 5/25 meter checks from the position.
- Caring for the wounded or performing medical evacuation (MEDEVAC).
- Expecting additional attacks and checking the area for other IEDs.
- Securing suspected evidence. (Evidence is those things that will help the intelligence community to identify the bomber or bomb maker. Evidence includes shrapnel, parts of detonation devices, and containers.)
- Talking to local witnesses. Obtaining names, pictures, and locations of personnel for follow-up interviews. Giving locals contact information for reporting suspicious activity.
- Continuing the mission.
- Conducting a comprehensive AAR.

RISK MITIGATION FOR CONVOYS

Note. These are broad generic suggestions. Refer to the most current convoy handbooks.

E-2. The five golden FP rules for convoys are—

- **Rule 1.** Be equipped to fight.
- **Rule 2.** Understand the threat.

- **Rule 3.** Know how to react to threat situations.
- **Rule 4.** Know where help is.
- **Rule 5.** Know how to ask for help.

E-3. There are three types of convoys and different reasons why the enemy would hit them. They are—

- **Long haul (replacement forces).** The enemy wants to initiate contact and try to get into your decision cycle first.
- **General support.** These are huge convoys carrying food, water, and numerous pilferable items that the enemy would like to capture for financial gain.
- **Local (brigade support area to the unit**). The enemy will try to capture equipment, slow down resupply operations (which slows down combat operations), and possibly continue to try and intimidate you to leave.

E-4. Every convoy should be treated as a combat operation. Units must follow or develop tactical convoy SOPs. Before conducting convoy operations, units must consider the following:

- **Predictability.** Do not set patterns. (Patterns are killing Soldiers and Marines. Developing patterns gives the enemy what he is looking for—a time and a place).
- **Contingency plans.** Ensure that contingency plans cover anything that can happen. Remember that what works in peacetime may not work in war. Cover, at a minimum, procedures for—
  - Vehicle preparation, vehicle hardening, gear preparation, maps/smart packs, load sheets.
  - A wreck, a flat tire, a stalled vehicle, a damaged vehicle, and so forth. Plan for self-recovery, to include alternate towing options (tow bars, tow straps, locally fabricated chains). Rehearse vehicle recovery. Attempt to have run flat tires and rims on all wheeled vehicles.
  - Debris removal.
  - Crowd control. (Crowds quickly gather around disabled vehicles and accidents. They can loot cargo and remove or strip the vehicles.)
  - Escalation of force procedures.
  - Encountering a sniper (with or without casualties).
  - IEDs (predetonation and postdetonation). Decide whether to stop the convoy or continue moving if an IED is located. (This will depend on if the IED was seen before the convoy entered through the kill zone or if the convoy was hit and the extent of vehicle damage.)
- **Troop-leading procedures and comprehensive rehearsals.** Execute TLP and comprehensive rehearsals. (Commanders should ensure convoys are organized to fight at all times. Convoys must rehearse reaction drills frequently in order to be able to fight as a cohesive team.)
- **Communications.** Ensure that—
  - A good communications plan for the convoy exists.
  - Every vehicle can communicate via a common method. (Have a backup communications method.) In dead zones (which can cover several miles), have a plan in case the convoy gets hit in one of those areas.
  - Everyone knows the combat network (COMNET) identification changes while moving through unit zones.
  - Everyone knows the frequencies for MEDEVAC and how to call them in.
  - Everyone knows how to call for fire and close air support (CAS).
- **Medical considerations.** Ensure that—
  - A plan for medical attention exists.
  - Everyone is trained on basic first aid.
  - Combat lifesavers (CLSs) or medics are in the convoy and their location is known by all.
  - Everyone knows the location of aid bags.
  - Aid bags are stocked.

E-5. During convoy operations, units must—

- Ensure that personnel wear all protective gear available, to include ballistic eye protection, goggles, Kevlar® helmets, body armor with plates, and hearing protection. Wear seatbelts when moving. During mounted movement, ensure that drivers, track commanders, and gunners have as much of their body inside the vehicle as possible to reduce the possibility of being struck by shrapnel or being exposured to the initial blast.
- Keep doors locked during movement to prevent vehicle occupants from being thrown from the vehicle during the initial blast or in the event of vehicle rollover.
- Keep windows down (unless windows are made of ballistic glass). Place polyester film on the windows if they are not made of ballistic glass.
- Drive with the daytime lights off. Try to make them appear as regular vehicles during hours of darkness.
- Ensure that Soldiers and Marines who are not driving are alert for suspicious activity and prepared to respond.
- Designate sectors of observation and fire. Ensure that a designated spotter uses binoculars during the daytime and thermal optics or night vision devices at nighttime. Try to use the same spotter whenever possible to increase the chances of noticing any changes on the route.
- Vary the separation distance between vehicles. Maintain an appropriate reaction time between vehicles.
- Consider the role of the vehicles in overwatch to support convoys.
- Drive at a safe/fast speed (35 miles per hour) based on the leadership, Soldier or Marine experience, and METT-TC factors. Do not be a steady target that allows the enemy to successfully engage you. Base a safe speed on factors such as the vehicle type, the weather, road conditions, time of day, and the driver experience.
- Consider driving in the center of the road and staying on the hardball to increase security and standoff.
- Avoid potholes, drainage holes, manhole covers, and overpasses where possible.
- Be extra cautious at choke points. Pay attention to the flanks for possible IED and VBIED attacks if anything causes the convoy to stop. Stay alert for vehicle breakdowns, vehicles entering roads, bridges, traffic jams, sharp turns, and so forth.
- Prevent civilians and civilian vehicles from entering convoys. Consider placing signs on convoy vehicles in the native dialects to warn civilians and motorists to stay away from the convoy and that failure to do so may result in deadly force to be used against them (depending on the ROE).
- Execute the 5- to 25-meter drill once the unit has come to a stop for longer than 1 minute.
- Be prepared to execute near and far ambush drills and to fight and maneuver against the enemy.

E-6. There are several different types of attacks involving IEDs and VBIEDs. These include basic, change of traffic, and multiple IEDs (Figures E-1 through E-3, page E-4).

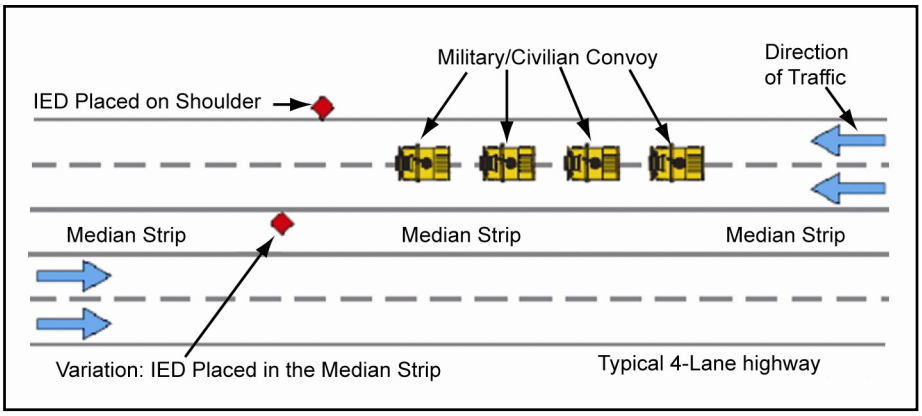

Figure E-1. Basic attack

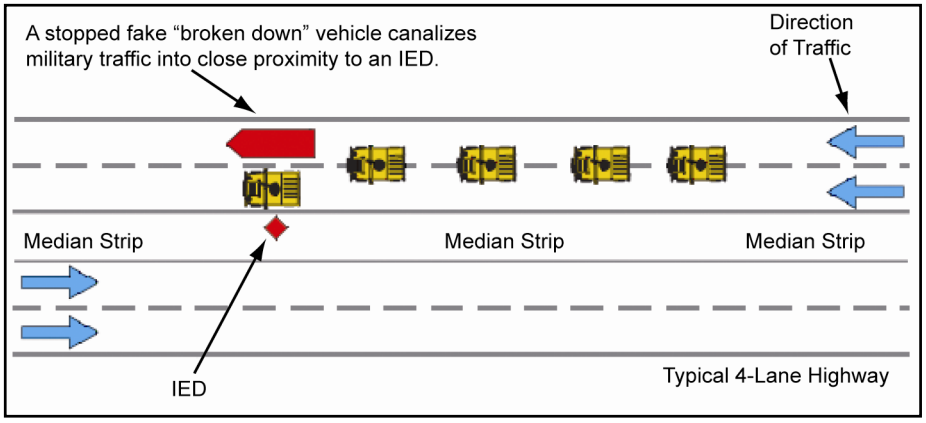

Figure E-2. Change of traffic attack

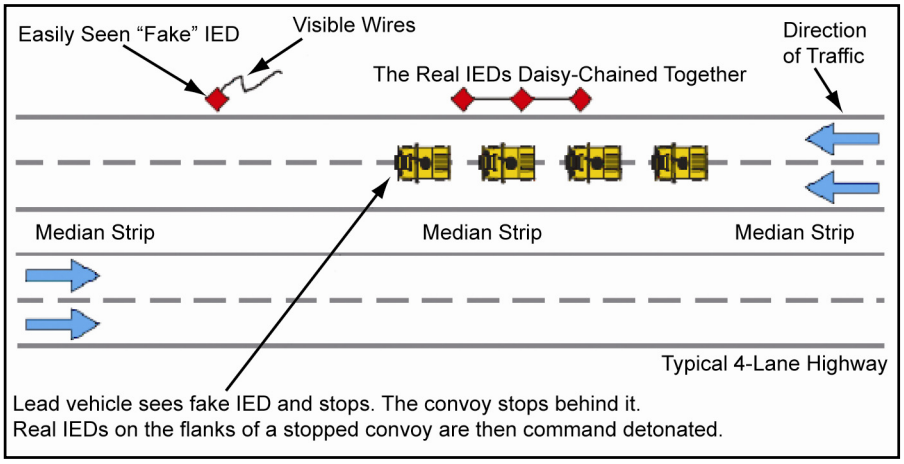

Figure E-3. Multiple IED attack

MOBILITY CORRIDORS

E-7. The mobility corridor (MC) is part of a layered and integrated security approach to LOC security. Layered security constitutes concentric rings that increase in survivability and response measures. The first ring (the center ring) being the ability of every convoy to defeat a Level I threat and to delay a Level II threat. The next ring (middle ring) provides the increased security/protection capability in support of the center ring activities, capable of defeating Level I and Level II threats, and supports the defeat of Level III threats. The middle ring is also capable of integrating fires, CAS, MEDEVAC, safe havens, vehicle removal/recovery operations, and so forth in support of the center ring and central effort that is the MC concept. The final ring (the outer most ring) is the final ring of protection and brings with it the ability to defeat all level of threats through the integration of all joint capabilities.

E-8. An MC is a protected LOC that connects two support areas within the battlespace. Within the MC are main and alternate roads, railways, and/or inland waterway supply routes used to support operations. Within an AO, there is an MC network that consists of multiple MCs that connect intertheater APOD and SPOD; intra-theater APOE and APODs; corps support, distribution, and storage areas; division support, distribution, and storage areas; and BCT support areas. While the support area is within the BCTs AO and responsibility, the supporting MC is the responsibility of the division. The BCT is responsible for tactical LOC operations and security beyond the BCT support area. The width and depth of an MC will be dependent on METT-TC factors and the guidance of the combatant commanders.

E-9. The establishment of an MC network is the result of applying multiple functions and establishing required command, control, and support relationships. The collective integration and synchronization of units, capabilities, and facilities will provide a comprehensive three-dimensional protection capability for the designated LOCs, the unit and convoy movements on the LOCs, and the units supporting LOC and movement operations. A fully developed MC will consist of military police units providing route regulation and enforcement, straggler and dislocated civilian control, area and route security, convoy escort, QRF, and logistical units conducting and managing movement control. Supporting functions include units and capabilities for vehicle recovery and storage, cargo transfer, refueling, road maintenance and repair, MC safe haven support facility construction and repair, CBNRE detection and response, aerial reconnaissance, and medical treatment and evacuation.

E-10. The constitution of an MC and the required units and capabilities to support MC operations are not new to the Army. What is new is the requirement to doctrinally codify a holistic, fully integrated and synchronized LOC and convoy protection system. The requirement to establish MC doctrine is based on the combination of, and the complexity resulting from a nonlinear asymmetrical battlespace, conducting threat-based operations with minimal regard for occupying terrain, combat forces by-passing up to company-sized mechanized forces, combating new categories of threat forces, smaller stockpiles with an anticipatory “push” logistics system, and conducting simultaneous major combat operations (MCO) and stability and reconstruction operations. The establishment of an MC network and the allocation of resources to conduct MC protection and support operations is a command function that must be synchronized with Army, joint, multinational, and HN forces supporting MC operations and the applicable movement control agencies.

E-11. The MC concept provides a solution to current and future force requirements for ground LOC movement as it pertains to a comprehensive approach to increasing the survivability of land forces in the conduct of full spectrum operations. This concept provides for continuous support in keeping the MC secure and operational, thus directly increasing the mobility, survivability, sustainability, and responsiveness of combat enablers in support of all operational effort. Further refinement to this concept and the DOTMLPF recommendations are required to ensure that the best solution and overall success is achieved in support of our Soldiers, sailors, airmen, and Marines of today and tomorrow.

This page is intentionally left blank.

Appendix F

Military Search

Military search operations are imperative to uncovering and neutralizing concealed enemies and devices. Friendly forces seize the initiative through offensive military search operations locating people, information, and material resources employed by the enemy and then acting to interdict the ability of the enemy to conduct operations. Friendly forces protect themselves and friendly populations against attack, in large part, through defensive military search operations. As a principle means of both carrying the fight to the enemy and of defending friendly forces, effective search operations are vital to success.

MILITARY SEARCH PRINCIPLES

F-1. The following principles are essential to a successful search mission:

- **Be systematic.** The approach to any search operation must be careful, deliberate, safe, detailed, and methodical to avoid oversight. The systematic search principle applies equally to the planning, coordination, and execution of all search operations.
- **Be flexible.** TTP and equipment must adapt to an evolving operational and tactical environment where the adversary constantly changes its methods of operations in an attempt to trap, deceive, mislead, or misdirect the searcher. All procedures should be considered to be flexible, but due consideration should be given to ensuring consistency while not compromising safety.
- **Be safe.** Achieve search safety by the mitigation of risk. Some examples include—
  - The minimum number of personnel operating in an area. Search pairs should operate with some sort of buffer zone between them and the next pair (for example, two rooms).
  - The minimum time on the target. If a suspect item is found, the minimum time should be spent obtaining the relevant details of the target.
  - The movement of things remotely to obtain a better view of a suspected device. If there is the slightest doubt about an item, it should be reported to EOD using the explosive hazard spot report.
  - The wait times (a waiting period). Wait times should be used after every positive action and should be varied to eliminate forming a procedural pattern.
  - Not picking anything up.
- **Minimize disruption and destruction.** Military search operations must both minimize the destruction of property and the disruption to the local population. This principle is important to maintaining the good will of the local population or at least minimizing the ill will generated. Commanders at all levels have a continuous responsibility to balance long-term physical and long-term psychological damage caused by search operations with the benefit gained. A policy must be considered for compensating searched individuals for any damage occurring during search operations.
- **Document.** Careful documentation ensures that search teams are correctly tasked, the search is controlled and thorough, and the maximum benefits are gained from the search.
  - **Isolation.** Cordon and protection are vital to any search task; the teams are not there to defend themselves against outside influence. The cordon to must maintain the sterility of interference by friendly forces.

- **Distractions.** Searchers must be free from distractions; search operations require the total attention of the participants. Leaders are to ensure that searchers are not distracted by visits of senior officers, the media, and so forth.
- **Command and Control.** C2 is vital to the conduct of the search and the coordination of the support, both military and civilian. Everybody must be informed of what is going on, especially civilian agencies.

F-2. The levels of search will be dictated by the threat. Searches are characterized by the following varying levels of thoroughness:

- **Basic search.** All military personnel must be prepared to conduct a basic search incidental to performing their assigned missions and duties on a continuing basis. A basic search does not involve a preplanned search operation and no specific enemy threats or environmental hazards have been identified. A basic search is inherent to FP. All military personnel must be able and ready to conduct a basic search.
- **Intermediate search.** An intermediate search is appropriate for deliberate, preplanned offensive search operations when there is no specific intelligence indicating the presence of functioning explosive or hazardous devices, there is no indication of environmental hazards, and a high assurance level is not required. Intermediate search is the first level at which units form teams to conduct search operations.
- **Advanced search.** An advanced search is appropriate for deliberate, preplanned search operations when there is specific intelligence indicating the presence of a functioning explosive or hazardous device, there are indications of environmental hazards, or a high assurance level is required.

F-3. Due to the many varied situations in which a search may be conducted, it is necessary to develop a set of guidelines within which to conduct a search. It should be noted that these procedures are only guidelines and may require adaptation to suit a particular task. The six standard search types are as follows:

- Person.
- Vehicle, incorporating vehicle checkpoints (VCPs).
- Area.
- Route.
- Nondisruptive building.
- Disruptive building.

F-4. A search operation may consist of one procedure or a series of related procedures, the application of which depends on the circumstances of the search. Therefore, it can be seen that, with the exception of safety measures, search procedures are not prescriptive to be followed lockstep. They must be adapted to meet the local situation. Search procedures must not become stereotyped, or the enemy will learn what to expect and take the appropriate evasive action.

IMPROVISED EXPLOSIVE DEVICE SEARCH AND DETECTION

F-5. The paragraphs below discuss the methods and principles of IED search and detection.

METHODS

F-6. Methods of IED search and detection, also known as IED hunting include—

- **Patrols.** Patrols should—
  - Conduct aggressive reconnaissance.
  - Use reconnaissance patrols to feed intelligence development.
  - Use specific objectives, such as people, places, or things.
  - Use security patrols to mitigate risk.
  - Treat every convoy as a combat operation.

- **Ambushes**. Ambushes should be used—
  - In locations of potential "high risk" IED emplacement areas.
  - By scout and sniper teams.
- **Raids.** Raids should—
  - Focus on specific targets when reliable, actionable intelligence is available.
  - Prepare to exploit the raid site with the appropriate intelligence collection assets, such as CEXC, EOD, search dogs, CID, and so forth.
  - Demonstrate to the enemy the certainty that you will act, but uncertainty as to when and where.
- **Proven TTP.** (TTP developed and used successfully by units.) When using TTP—
  - Do not confuse convoy procedures with IED search and detection.
  - Remember that TTP are situation driven and must be combined with principles of leadership.
- **Convoy escorts.** When performing a convoy escort—
  - Ensure that IED search and detection teams proceed ahead of the convoys.
  - Drive parallel to the MSR when possible. This tactic allows for a view from an additional vantage point. Always observe the area from the enemy perspective.

PRINCIPLES

F-7. Principles for IED search and detection, also known as IED hunting include—

- Knowing the AO and maintaining SU, soliciting information, and reviewing intelligence reports.
- Building experience in units. Traveling roads day after day. Observe routines and attitudes of the local populace. Using your experience on these routes will allow you to judge the attitude of the local populace (for example, if the town square is empty when it is normally full of people). Remember that these techniques will not work if you change personnel every day; the reason they work is because you have Soldiers and Marines who—
  - Know what the roads look like and can recognize when something is different.
  - Have gained experience by conducting multiple operations searching for IEDs.
- Concentrating efforts on high-threat areas. Targeting likely sites using the IPB process (battle tracking). Updating and clearing NAI at least once every 24 hours and varying the times constantly.
- Negating IEDs before they are emplaced, to include—
  - Capturing or killing the bomb makers, trainers, emplacers, and their leaders.
  - Finding and destroying explosive caches.
  - Interdicting enemy supplies.
  - Securing ordnance before it can be used to become an IED.
  - Operating at night or other known times of IED emplacement.
  - Investigating people performing roadside work or vehicle maintenance.
- Using optics, (binoculars, spotting scopes, and so forth) to view suspected IEDs from a distance; using every tool available.
- Patrolling with a high degree of unpredictability. Making U-turns; varying movement by time, routes, gates, convoy composition, mounted, and dismounted; and drive the wrong way on ramps. (Remember, we own the roads.)
- Driving in the center of the MSR at slow speeds (10 to 20 miles per hour) and scanning the surrounding areas. (It is difficult to detect anything driving at high speeds.) Remembering not to set patterns while conducting searches.
- Ensuring that upon arrival in the search area that actions are varied continuously (search should appear completely random). Driving in one direction for 1 or 2 miles, then making a U-turn, search the other direction, pick up, and move to a completely different AO. Being unpredictable

so as not to give the enemy a time and place; unpredictability makes it harder for the enemy to target IED search teams.

- Considering anything suspect that looks out of place (for example, a rock pile or brush, wire, detonating cord, an abandoned vehicle, symmetrical trash bags).
- Maintaining a visible presence and aggressive posture.
- Conducting mounted and dismounted surveillance between checkpoints.

WARNING

Do not attempt to do EODs job of neutralizing IEDs; what appears to be simple may indeed be complex.

ENTRY CONTROL POINT

F-8. ECPs are a likely target for VBIEDs. Before constructing an ECP, conduct an IPB identifying the specific threats to the installation. Identified threats are ECP design drivers.

DESIGN CHARACTERISTICS

F-9. ECP design characteristics include—

- **Deterrence.** The overall ECP design, security posture, and procedures should convey to a potential aggressor a hardened access point not likely to be penetrated—it will fail.
- **Detection.** Detection is the multiple measures that sense, validate, and communicate the presence of an aggressor to the response force (cameras, vehicle passes, searches, questioning, bomb dogs, and so forth).
- **Defense.** Defense is the active and passive measures employed to prevent an aggressor from gaining entry or to minimize the effects of an attack (drop barriers, blast walls, stand off, serpentines, guards, and so forth).
- **Defeat.** Defeat is the active and escalating measure of force design to defeat an aggressor (heavy machine guns (MGs), AT weapons, or QRF).

DESIGN ELEMENTS

F-10. ECP design elements include—

- **Traffic control.** The flow of vehicles and personnel must be effectively controlled in order to efficiently segregate and process legitimate movement through the ECP. Traffic control should be maintained by—
  - Segregating and conducting identification checks, HN police searches, and vehicle and personnel passes.
  - Using speed control (speed bumps or serpentines).
  - Using positive stops (wire rope barriers or vehicle drop barriers).
  - Channelizing and funneling traffic through the ECP provides clear engagement zones for MGs.
  - Allowing unauthorized vehicles to exit.
- **Threat mitigation.** Threat mitigation involves features (such as blast walls to protect from the effects of overpressure) to reduce identified threats and increased standoff distances to protect against fragmentation. Threat mitigation includes—
  - Hesco® barriers for blast protection (VBIED, suicide bomber, or direct and in-direct fire).
  - Predetonation screen (rocket-propelled grenade [RPG] attack).
  - Heavy MG and AT weapons (engage enemy vehicles or personnel).
  - Standoff to reduce effects from blast overpressure and fragmentation.

  - Potential VBIED (buses or trucks) should be restricted access and off-base trans-load yards should be used.
- **Procedures.** Operating procedures should be integrated so that all processes are thorough, quick, and done with some degree of redundancy.
- **Defense in depth.** Defense in depth is the repeated use engagement zones.
- **Threat mitigation.**
- **Host nation police.** HN police screen initial traffic.
- **Authorized vehicles moving to U.S. controlled zone.** The driver and passengers move to the identification and search area. The vehicle is searched without the driver or passenger observing. Explosive detection dogs are used.
- **Cleared traffic.** Cleared traffic continues through the ECP.

PERSONNEL AND VEHICLE SEARCH

F-11. A personnel and vehicle search includes—

- Using the two man rule when searching personnel (one searching and one covering).
- Using a separate search area from the holding area (allow for reaction).
- Removing and searching (separately) bulky clothing.
- Being thorough (occasionally test yourselves).
- Using the presence of an interpreter.
- Augmenting searches with handheld wands detectors, explosive sensors, and dogs.
- Allowing no locals to observe the vehicle being searched, if possible.

F-12. A variety of information sources should be used, including imagery assets, to establish predictable patterns the enemy will use when emplacing IEDs and ensure that it is updated daily. The enemy routinely reuses the site of previously successful IED attacks. To deny enemy emplacement of additional IEDs in this location, units must plan for the use of ISR assets to either capture or destroy enemy personnel emplacing the IEDs. These areas would become a NAI.

F-13. The latest HUMINT obtained from either MI or local nationals should be used. It is important to ensure that the information has been properly filtered to determine its reliability.

F-14. The most effective way to enhance security within the AOR in relation to the IED threat is to deny the enemy the opportunity to emplace IEDs. There are a variety of activities units can incorporate to accomplish this. Units must develop a good relationship and means of communicating with the local community so community members feel comfortable providing the unit with information. Examples include IO and techniques (such as advertising telephone numbers to report enemy activity within the area or to report locations of potential IED making materials) and media announcements and communications in the local dialects. When this information is provided, it is imperative that the unit ensures that the source of information remains anonymous. Unit HUMINT personnel should be consulted regarding the proper handling of information and the protection of sources.

F-15. Regular sweeps of an AO should be conducted to reduce the availability of bomb-making materials. This becomes necessary to reduce the amount of military explosives or ordnance.

F-16. Coordination with HN military or police forces can provide the unit with an increased HUMINT capability, local credibility, additional insight into the community, and so forth. Caution must be taken to ensure that operations security (OPSEC) is not compromised.

F-17. Methods of interdicting enemy activity include conducting presence patrols, observation points, and checkpoints. These methods deny the enemy access to key terrain for IED emplacement. Counter-IED-ambush teams and scout sniper teams can be employed to interdict or kill the enemy.

This page is intentionally left blank.

Appendix G

Specialized Equipment

In general, IED area clearance uses a combination of systems to survey an area contaminated with IEDs. An initial survey determines the type and net explosive weight of munitions they expect to encounter in the area. Detection uses personnel and equipment (Buffalo, AN/PSS-14, and so forth) to inspect the area for possible IEDs, which are then neutralized by EOD personnel. Proofing involves verifying that all explosive material is removed. Due to the unconventional nature of IEDs, it is almost impossible to "proof" an area of IEDs. Area clearance operations are extremely deliberate and require commanders to thoroughly understand the threat presented by the type of munitions they expect to encounter and the capabilities and limitations of the available equipment as a framework to guide their area clearance operation. Thorough planning and attention to detail is paramount to ensure that Soldiers and Marines are kept safe.

Note. See FM 20-32 for information on other specialized engineer equipment. See FM 4-30.5 for information on other specialized EOD equipment.

INTERIM VEHICLE-MOUNTED MINE DETECTOR

G-1. The complete Interim Vehicle-Mounted Mine Detector (IVMMD) System consists of one mine detection vehicle, one towing or mine detection vehicle, and three mine detection trailers. This kit comes with repair packs (referred to as "Red Packs") which contain spare detection arrays and front and rear assemblies. Each unit receiving two or more IVMMDs will also receive a third repair pack, called a "Blue Pack." This pack contains all of the major repair parts, such as axels, engines, and batteries. This system can clear single traffic routes at a rate of 85 kilometers (daylight only) per day. Figure G-1 shows a Meerkat and Figure G-2, page G-2, shows a Husky.

Figure G-1. Meerkat

Figure G-2. Husky

BUFFALO

G-2. The Buffalo (Figure G-3) is a heavy blast-resistant vehicle used for route clearance missions. The Buffalo protects the crew from the effects of blasts. The IVMMD and the Buffalo are highly effective. They are routinely used to sweep the shoulders of the route before movement. The Buffalo has an arm (Figure G-4) with mine detection capabilities, which is maneuvered by the vehicle operator from inside of the vehicle while it is in travel (Figure G-4). Soldiers and Marines use the hydraulic arm to search suspect areas along the route from inside the blast-protected vehicle.

Figure G-3. Buffalo

Figure G-4. Buffalo with a clearing arm extended

CASSPIR

G-3. The Casspir (Figure G-5) has been in use in South Africa for over 20 years. It is a four-wheeled armored vehicle used for transporting of troops. It can hold a crew of two, plus 12 additional Soldiers or Marines and associated gear. The Casspir is unique in design, and provides for passive mine defense. The main body of the vehicle is raised aboveground, so that if a mine is detonated, the explosion is less likely to damage the crew compartment and kill the occupants. The vehicle is also armored for added mine safety as well as protection from small arms fire.

Figure G-5. Casspir

MEDIUM MINE PROTECTIVE VEHICLE

G-4. The medium mine protective vehicle (Figure G-6) is a C-130 transportable medium blast-resistant transport vehicle. The system is used to transport combat and CS personnel conducting route clearing. In addition to these missions, the medium mine protective vehicle can be used for transporting very important persons (VIP). To conduct a thorough route clearance, units must employ the IVMMD, Buffalo, and medium mine protective vehicle as a package.

Figure G-6. Medium mine protective vehicle

COUGAR

G-5. The Cougar (Figure G-7, page G-4) hardened engineer vehicle (HEV) is a multipurpose, armored, mine-protected 12-ton vehicle. The design uses a monocoque capsule which protects the driver and crew

from small arms fire, mine blasts, and IEDs. Typical roles for the vehicle are mine-protected troop transport for security, stability, and peacekeeping missions; protected weapons platform; law enforcement special response vehicle; and an EOD and range clearance vehicle. The vehicle can accommodate 10 passengers in a 4 by 4 configuration and 16 passengers in a 6 by 6 configuration.

Figure G-7. Cougar

MINE-PROTECTED ARMORED DOZERS

G-6. The mine clearing armor protection (MCAP) kit (Figure G-8) includes all the necessary armor to protect the operator and critical components of D7G dozers from 7.62 millimeter, armor-piercing ammunition and antipersonnel (AP) mine blast fragmentation. The kits are bolted and pinned to a bulldozer and the existing frame assemblies of track-type tractors and hydraulic excavators. Mine clearing rakes can be attached to existing bulldozer blades, creating a 12-foot-wide path and a soil penetration depth of 12 to 18 inches. Both a light-soil and a heavy-soil blade are available. The MCAP is capable of mine and UXO clearing purposes in uneven, light or heavily vegetated terrain.

Figure G-8. MCAP dozer

G-7. The D-9R armored dozer (Figure G-9) is another route or area clearance asset available to commanders for use in maneuver operations. The dozer is capable of removing abandoned vehicles or suspected VBIEDs from roadsides. Its armored plating can withstand up to .50 caliber ammunition and serves as a protective measure to its operators. The dozer is also effective in removing rubble and debris from roadsides, demolishing buildings, and breaching strongpoints or defensive positions.

Figure G-9. D-9R armored dozer

ROBOTS

G-8. Small robotic systems are the primary EOD tool for remote operations to render safe and dispose of IEDs. They are also used to provide Soldiers and Marines with a standoff capability to avoid unseen dangers, thus keeping Soldiers or Marines outside the blast radius of explosive hazards.

G-9. Units will request EOD personnel to investigate suspected IEDs by using camera-carrying robotic platforms designed to convey real-time imagery to EOD personnel. These afford unit personnel with a safe method of verifying that the device is an IED. Figure G-10 shows an EOD robot.

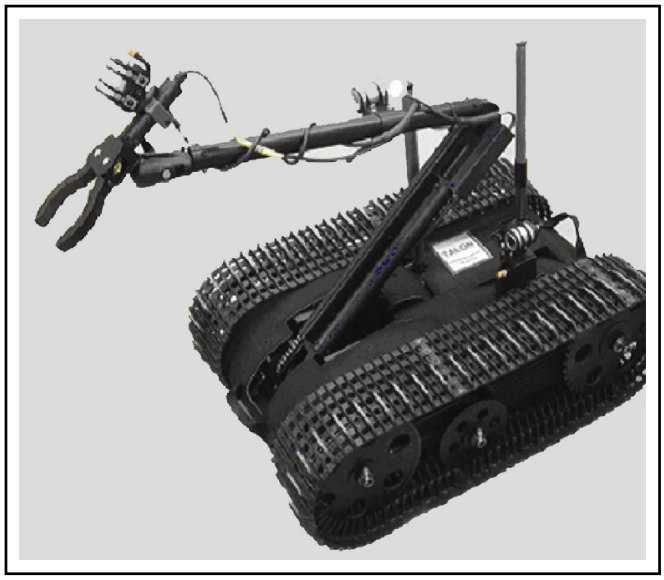

Figure G-10. EOD robot

SPECIALIZED SEARCH DOGS

G-10. To obtain the maximum value from the services of trained dogs, it is essential to have a sound understanding of the tactical situation and conditions best suited to their employment. Dogs, like the rest of the animal kingdom, are subject to outside influences that have a direct bearing on their behavior. Dogs can only be used after a careful appreciation of the tactical picture, climatic conditions, and the terrain has been made and found favorable.

G-11. A specialized search dog (Figure G-11, page G-6) is trained for route and area, building (occupied, unoccupied, or derelict), and vehicle search. The specialized search dog searches for and indicates to its handler the presence of all firearms, ammunition, explosives, and other materials relating to bomb-making

equipment or explosive hazards. Dog teams are capable of searching all types of urban and rural environments and can locate both fresh and long-term hides (mines and explosives) constructed of a variety of materials. Dogs are a quick and reliable method for checking an area. They can work at night, but enough artificial light is required to enable the handler to see the dog working and the immediate surrounding area.

Figure G-11. Specialized search dogs

G-12. Specialized search dog teams, when deployed correctly, can minimize the risk of life to friendly force personnel. They can be used when other forms of detection fail. The specialized search dog works off leash and out ahead of its handler, minimizing risk to its handler and other Soldiers and Marines on the mission. These dogs have a high degree of public acceptance since they are not attack-trained and are family friendly breeds (such as a Labrador or a Spaniel). The dogs are not influenced by factors that affect human opinions. They should be bold, but not aggressive, and steady under gunfire. They are of limited use to search personnel. The dogs may tire during extended searches (if working 40 minutes an hour for about 6 hours). Much of their value is negative, that is, if they show no interest, there are unlikely to be any weapons or explosives in the search area. The specialized search dog will—

- Search for firearms, ammunition, explosives, hides, and bomb-making equipment in—
  - Buildings that are occupied, unoccupied, or derelict.
  - Vehicles (cars, trucks, trains, ships, boats, or aircraft).
  - Open areas (fields, islands, woods, hedgerows, or embankments).
  - Route clearance (roads, tracks, or railways).
- Check buildings after workmen have left, search AOs, such as VCPs and helicopter landing zones (HLZs). These dogs are used to search buildings and areas immediately before VIP visits in-theaters.

G-13. See ST 20-23-10 for specialized search dog operations.

HANDHELD DETECTORS

G-14. The AN/PSS-14 is a single-Soldier-operated handheld mine detector (Figure G-12) that integrates a state-of-the-art metal detector with compact ground-penetrating radar (GPR) into a lightweight handheld system (about 11 pounds with batteries). Only one standard issue Army battery (BB-390A/U) is used to power the AN/PSS-14. The AN/PSS-14 is capable of detecting metallic and low-metallic AP and AT mines in on-road and off-road conditions. Sensor fusion and sophisticated algorithms reduce the false alarm rate that current metal detectors experience in cluttered metal environments.

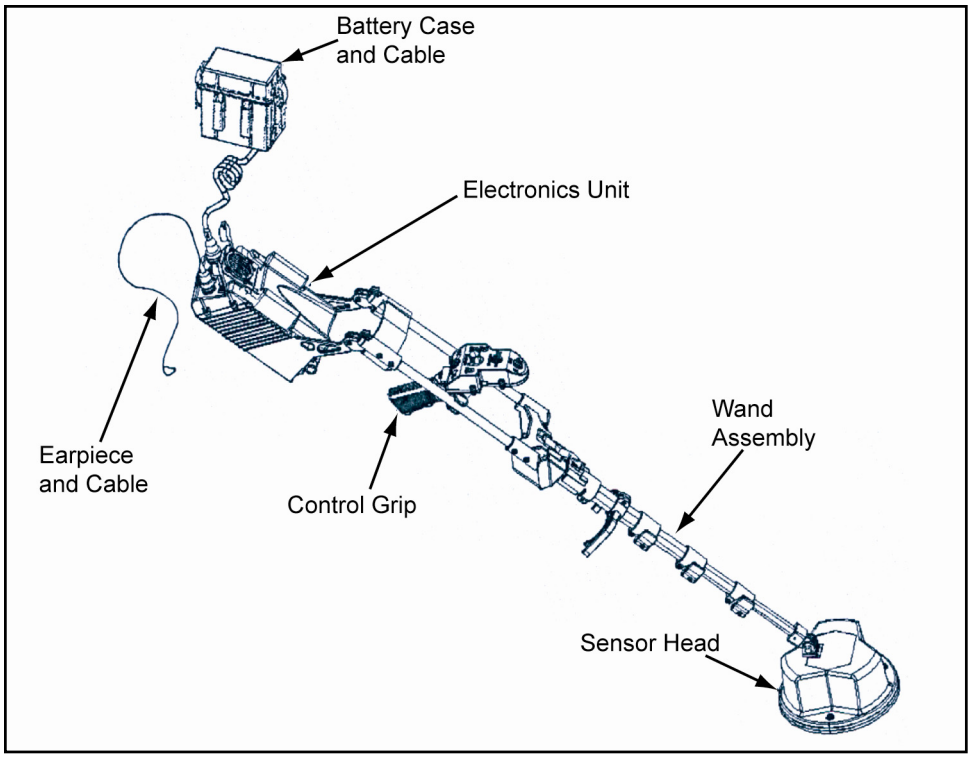

Figure G-12. AN/PSS-14 mine detector

G-15. Handheld explosive sniffers (Figure G-13) draw air through a detector nozzle/valve, which determines the presence of several types of common explosive chemicals. Several of these detectors are reliable in detecting traces of explosives on packaging materials or even residue on individual's hands or clothing. Several companies produce these detectors (handheld explosive sniffers and explosives residue detection sprays), which are available as commercial off-the-shelf (COTS) purchases.

Figure G-13. Handheld explosive sniffer

SEARCH KIT

G-16. A wide variety of tools and equipment are available to assist in a search. The provision of the right tools and equipment enables searches to be conducted effectively and time will be saved and damage to property minimized. To ensure safety and efficiency, users must be trained on and practice the use of this type of equipment.

G-17. The purchase of equipment should be considered far in advance of any search operation. Trial units must be given a great deal of notice to enable the acquisition of a cross section of materials, such as explosives and facilities and venues.

G-18. Equipment is not infallible and is only an aid to search. When possible, two different pieces of equipment that are based on different technologies should be used.

INVESTIGATION EQUIPMENT

G-19. Investigation equipment includes (Figure G-14)—

- An explosive detection kit.
- A handheld metal detector.
- An extendable lit mirror.
- An extendable pole.
  - One with a small mirror.
  - One with a large mirror.
- A mine probe.
- A distance finder.
- A nonmagnetic fork.
- A nonmagnetic trowel.
- A pruning saw.
- A scrub cutter.
- Two small flashlights.
- A laser pointer.
- A bore scope.
- A 17-piece bit set.
- A cordless drill.

MARKING EQUIPMENT

G-20. Marking equipment includes a route marking system (40 white or 20 red), a mine bonnet, and an antitamper security seal. See Figure G-14.

REMOTE-ACCESS EQUIPMENT

G-21. Remote-access equipment includes (Figure G-14)—

- A 3.5 millimeter Kevlar line, to include a—
  - Fifty-meter reel.
  - One hundred-meter reel.
- A pulling handle.
- Carabiners. Carabiners and related equipment include—
  - Two screw gates.
  - Five integral pullies.
  - Ten screw eye self taps.
- Pitons (two large and two small).
- Hooks. Hooks required include—
  - Two single tangs.
  - Four double tangs.
  - Four 25-millmeter eyes.
- A self-opening snatch block.
- Two self-locking grips.

- Two shock cords.
- A spring-loaded clamp.
- Two wire slings.

ACCESS EQUIPMENT

G-22. Access equipment (Figure G-14) includes a Biel Tool® and an anel remover.

Figure G-14. Access equipment in the search kit

This page is intentionally left blank.

Appendix H

Training Resources

This section is a compilation of all training information on IED defeat. These resources are broken down into tasks, training aids, references, and courses.

TASKS

H-1. Individual tasks available on the Reimer Digital Library at <http://www.adtdl.army.mil> include—

- Common Task Training (CTT) 171-300-0016, Conduct a Presence Patrol, Version 1.1. 1 February 2005.
- CTT 191-379-4407, Plan Convoy Security Operations. 1 February 2005.
- CTT 052-192-1269, Detect Explosive-Hazard Indicators By Visual Means (TSP 093-401-5050).
- CTT 052-192-1242, Locate Mine and Booby Trap Indicators by Visual Means. 31 August 2003.
- CTT 093-401-5040, React to Unexploded Ordnance Hazards. 31 August 2003.

H-2. Center for Army Lessons Learned (CALL) and IED TF/staff articles are available at <http://call.army.mil> and include—

- Focused Intelligence.
- Understanding the Enemy.
- What Does a Commander Owe His Staff.
- Training Strategy. June 2004.
- Training Strategy narrative.

H-3. Leader related articles available from CALL/IED TF at <http://call.army.mil> include—

- Conducting Realistic Training.
- Convoys Are Combat.
- Fundamentals of Warfighting.
- Terrorist and You.

COLLECTIVE TASKS

H-4. Collective tasks available on the Reimer Digital Library at <http://www.adtdl.army.mil> include—

- Task 05-2-3091, React to a Possible Ground-Emplaced Improvised Explosive Device (IED).
- Task 05-1-1006, Prepare for Ground-Emplaced Improvised Explosive Device (IED) Defeat Operations Prior to Movement.
- Task 05-3-0407 (*), Perform an Engineer Reconnaissance (Training Support Package [TSP] 093-401-5050).

H-5. CALL products available from CALL/IED TF/articles at <http://call.army.mil> include—

- Newsletters 1 through 21, Iraq, Afghanistan 1 and 2.
- Various articles relating to IEDs, convoys, and so forth.
- Support to Deploying Units.
- TTP, Company, Battalion, Brigade, Staff Briefings.
- Warfighting, Operation Iraqi Freedom, Operation Enduring Freedom.
- Up-to-date articles of Operation Iraqi Freedom and Operation Enduring Freedom.

H-6. Available on the Reimer Digital Library, Commandant Approved Training, TSP Section at <http://www.adtdl.army.mil> includes—

- TSP 55-Z-0001, Convoy Survivability, Version 1.1. 27 August 2004.
- TSP 55-Z-0001-EX, Convoy Life Fire Exercise, Version 1.1. 27 August 2004.
- TSP 052-21B10D020, Detect Explosive-Hazard Indicators by Visual Means. 23 July 2004.
- TSP 093-401-5050, React to A Possible Improvised Explosive Device (IED). 21 May 2004.
- TSP 071-T-3412, Force Protection. 7 March 2003.
- TSP 071-T-1003, Secure a Route. 7 March 2003. (Geared to Bosnia, but presents valid points for OIF/OEF.)
- TSP 159-O-0301, Opposing Force: Paramilitary and Nonmilitary Organizations and Tactics. 1 June 2003.
- TSP 159-O-0001, Overview to a Military Guide to Terrorism in the Twenty-First Century. 12 October 2004.

H-7. Fort Polk/Joint Readiness Training Center situation training exercise training and evaluation outlines include—

- Conduct Cordon and Search in a Built-Up Area.
- Conduct Patrol Operations.
- Conduct Urban Area Reconnaissance.
- Establish Checkpoints or Roadblocks.
- Conduct a Convoy Escort.
- Conduct a Route Reconnaissance.
- React to Civil Disturbance Operations.
- Secure Routes.
- React to Sniper.
- Search a Building.

TRAINING AIDS

H-8. GTA, CJTF-7, and multinational corps IED products are available from CALL/IED TF/training at <http://call.army.mil> include—

- GTA 90-01-001, Improvised Explosive Device (IED) and Vehicular Borne Improvised Explosive Device (VBIED) Smart Card. 20 May 2004.
- GTA 90-01-003, Vehicle Search Techniques Smart Card. 6 August 2004.
- GTA 90-01-004, Logistics Convoy Operations Smart Card. 1 September 2004.
- GTA 05-10-044, Mine Awareness (SANDI). 1 May 1999.
- GTA 09-12-001, Unexploded Ordnance (UXO) Procedures. 3 January 1992.
- GTA 09-12-004, IED and VBIED Smart Card. 3 May 2004.
- GTA 07-01-038, Infantry Leader's Reference Card. January 1995.
- CJTF-7 Operation Enduring Freedom Smart Card 1, Report Procedures. 10 January 2004.
- CJTF-7 Operation Enduring Freedom Smart Card 2, Convoy Operations (Logistics). January 2004.
- CJTF-7 Operation Enduring Freedom Smart Card 3, Convoy Operations (Combat). 10 January 2004.
- CJTF-7 Operation Enduring Freedom Smart Card 4, IED and VBIED Threat. 10 January 2004.
- CJTF-7 Operation Enduring Freedom Smart Card 5, Vehicle Search Techniques. 5 January 2004.
- CJTF-7 Operation Enduring Freedom, IED Handbook. May 2004.
- Multinational Corps IED Smart Cards. 27 October 2004.

H-9. A video available on the Reimer Digital Library at <http://www.adtdl.army.mil> is Television Tape (TVT) 5-159, Improvised Explosive Device (IED) Awareness. 1 August 2004.

H-10. IED simulators available from the United States Army Engineer School include Training Aids for Possible Improvised Explosive Devices, <www.wood.army.mil/cehc>.

REFERENCES

H-11. SIPRNET Web Sites include—

- NGIC Energetics: <http://ngic.army.smil.mil/functionpgs/energetics/ied_resource.html>.
- U.S. Army INSCOM IED Threat: <http://dadpm.inscom.army.smil.mil/CENTCOM/ied_threat.asp>
- Central Command (CENTCOM): <hqsweb03.centcom.smil.mil/index.asp>.
- Joint IED Defeat TF: <https://releasable.portal.inscom.army.smil.mil/jieddtf/operations/default.aspx>.
- DA IED TF: <www.portal.inscom.army.smil.mil/jieddtf/default.aspx>.
- 82d Infantry Division (ID): <www.portal.inscom.army.smil.mil/82abn/default.aspx>.
- 4th ID: <http://www.portal.inscom.army.smil.mil/4thueyg2/default.aspx>.
- DIA: <http://www.dia.smil.mil>.
- DA Deputy Program Manager (DPM): <http://dadmp.inscom.army.smil.mil/CENTCOM/ied threat.asp>.
- NGIC: <http://www.ngic.army.smil.mil>.
- Multinational Corps-Iraq (MNC-I): <http://spsan.iraq.centcom.smil.mil/default.aspx>.
- MNC-I Explosive Hazard Coordination Cell: <http://spsan.iraq.centcom.smil.mil/C17/C7%20EHCC/default.aspx>.
- CEXC: <http://intel.socom.smil.mil/sojicc/frame.asp>.
- Joint EOD Tech Support Center: <http://tsc.jeodnet.smil.mil>.
- Combined Joint Task Force (CJTF)-7 Lessons Learned: <http://148.35.250.12/Sections/g3/Lessons Learned/IED/Friendly.>
- CALL Web Site: <https://call2.army.mil/ied_tf/ied_tf.asp>.
  - Warfighting-Joint IED Defeat Task Force.
  - Support to Deploying Units.
  - Newsletters.
  - Articles.

H-12. A Nonsecure Internet Protocol Router Network (NIPRNET) Web Site at <http://call.army.mil/> includes—

- CALL/IED TF/Training, Convoy Leader Handbook Revision V. 15 September 2004.
- CALL Handbook No. 05-11, Ranger Tactics, Techniques, and Procedures for OIF/OEF.
- CALL Handbook No. 04-24, Combat Convoy Handbook-CALL Handbook List.
- CALL Handbook No. 04-27, USSOCOM Convoy Leader Training Handbook.
- CALL Handbook No. 04-16, Cordon and Search Handbook.
- CALL Handbook No. 04-14, Effects-Based Operations Brigade to Company Level.
- CALL Handbook No. 03-35, Operation Enduring Freedom Handbook II.
- CALL Handbook No. 03-34, Mission Rehearsal Exercise.
- CALL Handbook No. 03-6, Tactical Convoy Operations. March 2003.
- CALL/Products/NFTF, November-December 2004.
- CALL/Products/Culture, Cultural Awareness Publications and Information OIF/OEF.
- Joint Readiness Training Center (JRTC), Convoy Leader Handbook.

H-13. FMs available on the Reimer Digital Library at <http://www.adtdl.army.mil> include—

- FM 21-16/MCWP 3-17.3, Unexploded Ordnance (UXO) Procedures. 30 August 1994.
- FM 20-32, Mine/Countermine Operations. 29 May 1998.
- FMI 3-07.22, Counterinsurgency Operations. 1 October 2004.
- FM 3-90, Tactics. July 2001.
- FM 55-30, Army Motor Transport Units and Operations. 27 June 1997.
- FM 3-07 (100-20), Stability Operations and Support Operations. 20 February 2003.
- FM 3-13 (100-6), Information Operations: Doctrine, Tactics, Techniques, and Procedures. 28 November 2003.
- FM 4-30.5, Explosive Ordnance Disposal Operations.28 April 2005.
- FM 20-32, Mine/Countermine Operations. 29 May 1998.
- FM 3-100.38, Multi-Service Procedures for Unexploded Ordnance.
- FM 34-54, Technical Intelligence. 30 January 1998.
- FM 3-11.20, Technical Escort Operations.
- FM 3-11.24, CBRNE for Environmental Reconnaissance.
- FM 4-30.16, EOD Multiservice Procedures for Explosive Ordnance Disposal in a Joint Environment. 15 February 2001.

H-14. Training circulars (TC) and STs available on the Reimer Digital Library at <http://www.adtdl.army.mil> include—

- TC 20-32-5, Commander's Reference Guide: Land Mine and Explosive Hazards (Iraq). February 2003.
- TC 9-21-01, Soldiers Improvised Explosive Device (IED) Awareness Guide Iraq and Afghanistan Theaters of Operation. May 2004.
- ST 20-23-10, Use of Specialized Search Dogs in Military Operations. February 2004.
- ST 20-23-8, Use of Demining Dogs in Military Operations. September 2003.

H-15. Media compact disks (CDs) available at <http://iedtaskforce.army.smil.mil> include—

- Joint IED Defeat Task Force Train the Trainer.
- Joint IED Defeat Task Force Field Team Products.
- Joint IED Defeat Task Force IED Training Version 2

COURSES

H-16. Courses available from CEHC at <http://www.wood.army.mil/CEHC> include—

- Explosive Hazards Awareness Training (EHAT).
- Explosive Hazards Awareness Train-the-Trainer (EHAT-T).
- Engineer Specific Countermine Training (ESCT).
- Engineer Specific Countermine Train-the-Trainer (ESCT-T).
- Counter Booby Trap Course (CBTC).
- Search Course.
- EHDB Training.
- MEOICC Training.
- Matilda Robot Training.

H-17. Courses available for the Ordnance Munitions and Electronic Maintenance School (OMEMS) are located at <http://omems.redstone.army.mil>. The primary OMEMS course if 2E-F231/030-F14.

H-18. Courses available on the Reimer Digital Library at <http://www.adtdl.army.mil> include the 553G-NG0021-A553 D01 Virtual Mission Preparation Course Conduct Escort of a Convoy. 8 June 2004.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

5-Cs	confirm, clear, call, cordon, and control
AAR	after-action review
ABCS	Army Battle Command System
ACP	access control point
AD	armored division
AFTTP	Air Force tactics, techniques, and procedures
ANFO	ammonium nitrate (fertilizer) fuel oil
AO	area of operations
AOIR	area of intelligence responsibility
AOR	area of responsibility
AP	antipersonnel
APOD	aerial port of debarkation
APOE	aerial port of embarkation
AR	Army regulation
ARNG	Army National Guard
ARNGUS	Army National Guard of the United States
ASCOPE	areas, structures, capabilities, organizations, people, and events
ASTAMIDS	Airborne Standoff Minefield Detection System
AT	antitank
ATTN	attention
AWG	Asymmetric Warfare Group
BATF	Bureau of Alchol, Tobacco, and Firearms (U.S.)
BCT	brigade combat team
BDA	battle damage assessment
bde	brigade
bn	battalion
BOS	battlefield operating systems
C2	command and control
C2PC	command and control personal computer
CA	civil affairs
CALL	Center for Army Lessons Learned
CAS	close air support
CASEVAC	casualty evacuation
CB	chemical and biological
CBR	chemical, biological, or radiological
CBIRF	United States Marine Corps Chemical Biological Incident Response Force

CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosive
CBTC	counter booby trap course
CCIR	commander's critical information requirement
CD	compact disk
CEA	captured enemy ammunition
CEHC	Counter Explosive Hazards Center
CENTCOM	Central Command
CEXC	Combined Explosives Exploitation Cell
CFLCC	Coalition Forces Land Component Command
CGS	common ground station
CI	counterintelligence
CITP	counter-improvised explosive device targeting program
CJTF	combined joint task force
CLS	combat lifesaver
CMEC	Captured Material Exploitation Center
CMOC	Civil-Military Operations Center
co	company
COA	course of action
COB	civilians on the battlefield
COE	contemporary operational environment
COMINT	communication intelligence
COMNET	combat network
CONUS	continental United States
COP	common operational picture
COTS	commercial off-the-shelf
CP	command post
CPA	Coalition Provisional Authority
CQM	close quarters marksmanship
CREW	counter radio-controlled improvised explosive device electronic warfare
CS	combat support
CSS	combat service support
CT	counterterrorism
CTC	Combat Training Center
CTT	common task training
D3A	decide, detect, deliver, and assess
DA	Department of the Army
DC	District of Columbia
DF	direct fire
DIA	Defense Intelligence Agency
DOD	Department of Defense

DOTLD	Directorate of Training and Leader Development
DOTMLPF	doctrine, organization, training, materiel, leadership, personnel, and facilities
DPM	Deputy Program Manager
DSN	defense switched network
DTES	Division Tactical Exploitation System
DTG	date-time group
E-5	sergeant
EAC	echelons above corps
ECP	entry control point
EHAT	explosive hazards awareness training
EHCC	explosive hazards coordination cell
EHCT-T	explosive hazards awareness train-the-trainer
EHDB	explosive hazards database
EHT	explosive hazards team
ELINT	electronic intelligence
EMF	engineer mission force
engr	engineer
EOCA	explosive ordnance clearing agent
EOD	explosive ordnance disposal
ERDC	Engineer Research and Development Center
ESCT	engineer specific countermine training
ESCT-T	engineer specific countermine train-the-trainer
EU	electronics unit
EXEVAL	exercise evaluation
fax	facsimile
FBCB2	Force XXI battle command-brigade and below
FBI	Federal Bureau of Investigation
FISINT	foreign instrumentation signals intelligence
FM	field manual
FMI	field manual interim
FMIG	Foreign Materiel Intelligence Group
FMFM	Fleet Marine Force Manual
FMT	forward maintenance team
FOB	forward operating base
FORSCOM	Forces Command
FP	force protection
FRAGO	fragmentary order
freq	frequency
ft	feet; foot
G-2	Assistant Chief of Staff, Intelligence

G-3	Assistant Chief of Staff, Operations and Plans
G-6	Assistant Chief of Staff, Command, Control, Communications, and Computer Operations (C4 Ops)
GBS	Global Broadcast System
GIS	geographic information system
GMFDB	global minefield database
gov	government
GPR	ground-penetrating radar
GRCS	guardrail common sensor
GSR	ground surveillance radar
GSTAMIDS	Ground Standoff Mine Detection System
GTA	graphic training aid
HEV	hardened engineer vehicle
HLZ	helicopter landing zone
HMMWV	high-mobility, multipurpose wheeled vehicle
HN	host nation
HOC	human intelligence operations center
htm	hypertext markup
http	hypertext transfer protocol
HQ	headquarters
HQDA	Headquarters, Department of the Army
HUMINT	human intelligence
HVTL	high-value target list
hwy	highway
I&W	indications and warning
ICDC	Iraqi Civil Defense Corps
ICDT	integrated capabilities development team
ICP	incident control point
ID	identification; infantry division
IED	improvised explosive device
IMAS	international mine action standard
IMINT	imagery intelligence
IMT	individual movement techniques
info	information
INSCOM	Intelligence and Security Command
INTS	intelligence surveillance
INTSUM	intelligence summary
IO	information operations
IPB	intelligence preparation of the battlefield
IPT	integrated product team
ISR	intelligence, surveillance, and reconnaissance

IVMMD	interim vehicle-mounted mine detector
IW	information warfare
JCMEC	Joint Captured Material Exploitation Center
JDIGS	Joint Digital Incident Gathering System
JIEDD	joint improvised explosive device defeat
JIM	joint, interagency, and multinational
JIPT	Joint Integrated Product Team
JOA	joint operations area
JP	joint publication
JRTC	Joint Readiness Training Center
JSAG	joint senior advisory group
JSLIST	joint services lightweight integrated-suit technology
J/STARS	Joint Surveillance Target Attack Radar System
JTF	joint task force
KIA	killed in action
km	kilometer(s)
L-V-C	live-virtual-constructive
LAN	local area network
LOC	lines of communication
LP	listening post
LRCT	long-range cordless telephone
m	meter(s)
MAC	Mobility Augmentation Company
MAG	magnetic
MANSCEN	Maneuver Support Center
MASINT	measures and signatures intelligence
MC	mobility corridor
MCAP	mine clearing armor protection
MCIA	Marine Corps Intelligence Activity
MCIP	Marine Corps information publication
MCO	major combat operations
MCOO	modified combined-obstacle overlay
MCRP	Marine Corps reference publication
MCS	manuever control system
MCS-ENG	Manuever Control System-Engineer
MCWL	Marine Corps Warfighting Laboratory
MDA	map decision aids
MDMP	military decision-making process
ME	maneuver enhancement
MEDEVAC	medical evacuation
MEOICC	Mine and Explosive Ordnance Information and Coordination Center

METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MG	machine gun
MI	military intelligence
MIL-STD	military standard
mil	military
min	minimum
MITT	mobile integrated tactical terminal
MLRS	Multiple Launch Rocket System
mm	millimeter(s)
MOPP	mission-oriented protective posture
MOS	military occupational specialty
MOUT	military operations in urban terrain
mph	miles per hour
MSR	main supply route
MTI	moving target indicator
MTOE	modified table of organization and equipment
MTP	mission training plan
MWR	morale, welfare, and recreation
NAI	named area of interest
NAVEODTECHDIV	Naval Explosive Ordnance Disposal Technology Division
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCO	noncommissioned officer
NCOIC	noncommission officer in charge
NGIC	National Ground Intelligence Center
NGO	nongovernmental organization
NIPRNET	Nonsecure Internet Protocol Router Network
NMAA	National Mine Action Authority
No.	number
NTTP	Navy tactics, techniques, and procedures
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment
OCONUS	outside continental United States
OE	operational environment
OEF	Operation Enduring Freedom
OIC	officer in charge
OIF	Operation Iraqi Freedom
OMEMS	Ordnance Munitions and Electronic Maintenace School
OMT	operational management team
OPFOR	opposing force

OPORD	operation order
ops	operations
OPSEC	operations security
OSHA	Occupational Safety and Health Administration
OPTEMPO	operating tempo
PA	public affairs
PCI	precombat inspection
PIR	priority information requirements
PMS	portable monitoring set
QRF	quick reaction force
QSTAG	Quadripartite Standardization Agreement
R&D	research and development
RCIED	radio-controlled improvised explosive device
RDE-L	rapidly deployable earthmoving (light)
RDE-M	rapidly deployable earthmoving (medium)
REF	Rapid-Equipping Force
REMBASS	Remotely Monitored Battlefield Surveillance System
RISTA	reconnaissance, intelligence, surveillance, and target acquisition
ROE	rules of engagement
RON	remain over night
ROVER	remote operations video enhanced receiver
RP	release point
RPG	rocket-propelled grenade
RSOI	reception, staging, onward-movement, and integration
RSP	render-safe procedure
rte	route
S-2	intelligence staff officer
S-3	operations staff officer
S-5	civil-military operations officer
S-6	command, control, communications, and computer operations (C4 Ops) officer
SANDI	stop, access, note, draw back, and inform
SCATMINE	scatterable mine
SBCCOM	Soldier and Biological Chemical Command (U.S. Army)
SIGINT	signals intelligence
SIPRNET	Secure Internet Protocol Router Network
SITTEMP	situational template
SME	subject matter expert
SMS	sensor monitoring set
SMUD	standoff munitions disruption
SOF	special operations forces

SOP	standing operating procedure
SPOE	sea port of embarkation
SPOD	sea port of debarkation
SSS	sensor signal simulator
ST	special text
STANAG	Standardization Agreement
STP	Soldier training publication
STX	situational training exercise
SU	situational understanding
TC	training circular
TCP	traffic control point
TDA	tactical decision aid
tech	technical
TECHINT	technical intelligence
TENCAP	tactical exploitation of national capabilities
TES	Tactical Exploitation System
TF	task force
THT	tactical human intelligence team
TLP	troop-leading procedures
TM	technical manual
TNT	trinitrotoluene
TOC	tactional operations center
TO&E	table of organization and equipment
TRADOC	United States Army Training and Doctrine Command
TSP	training support package
TSWG	Technical Support Working Group
TTP	tactics, techniques, and procedures
TVT	television tape
UAV	unmanned aerial vehicle
UIC	unit identification code
U.S.	United States
USAMC	United States Army Materiel Command
USAR	United States Army Reserve
USS	United States ship
USMC	United States Marine Corps ()
UXO	unexploded ordnance
VBIED	vehicle-borne improvised explosive device
VCP	vehicle checkpoint
VIP	very important person
w/	with
WIA	wounded in action

WIT	weapons intelligence team
WMD	weapons of mass destruction
www	World Wide Web

SECTION II – TERMS

booby trap

(DOD) An explosive or nonexplosive device or other material, deliberately placed to cause casualties when an apparently harmless object is disturbed or a normally safe act is performed (JP 1-02).

captured enemy ammunition

CEA is all ammunition products and components produced for or used by a foreign force that is hostile to the United States (that is or was engaged in combat against the United States) in the custody of a U.S. military force or under the control of a DOD component. The term includes confined gaseous, liquid and solid propellants, explosives, pyrotechnics, chemical and riot-control agents, smokes and incendiaries (including bulk explosives), chemical warfare agents, chemical munitions, rockets, guided and ballistic missiles, bombs, warheads, mortar rounds, artillery ammunition, small arms ammunition, grenades, mines, torpedoes, depth charges, cluster munitions and dispensers, demolition charges, and devices and components of the above. CEA can also include NATO or U.S. manufactured munitions that may not have been under U.S. custody or control.

combat system

A combat system is the "system of systems" that results from the synergistic combination of five basic subsystems that are interrelated to achieve a military function: combat forces, combat support forces, logistics forces, C2, and RISTA.

complex terrain

This is a topographical area consisting of an urban center larger than a village and/or of two or more types of restrictive terrain or environmental conditions occupying the same space. (Restrictive terrain or environmental conditions include but are not limited to slope, high altitude, forestation, severe weather, and urbanization.) Complex terrain, due to its unique combination of restrictive terrain and environmental conditions, imposes significant limitations on observation, maneuver, fires, and intelligence collection.

defeat

(Army) A tactical mission task that occurs when an enemy force has temporarily or permanently lost the physical means or the will to fight. The defeated force's commander is unwilling or unable to pursue his adopted course of action, thereby yielding to the friendly commander's will, and can no longer interfere to a significant degree with the actions of friendly forces. Defeat can result from the use of force or the threat of its use (FM 1-02).

***explosive hazard**

(Army) An explosive hazard is any hazard containing an explosive component. All explosive hazards currently encountered on the battlefield can be broken down into five categories: UXO, booby traps, IEDs, CEA, and bulk explosives.

explosive ordnance

(DOD) All munitions containing explosives, nuclear fission or fusion materials, and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket, and small arms ammunition; all mines, torpedoes, and depth charges; demolition charges; pyrotechnics; clusters and dispensers; cartridge and propellant actuated devices; electro-explosive devices; clandestine and IEDs; and all similar or related items or components explosive in nature (JP1-02).

improvised explosive device

(DOD) A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. Also called IED (JP 1-02).

***improvised explosive device hunting**

(Army/Marine) A counter-IED operation to proactively locate IEDs and the personnel who make and emplace them before the IED is detonated. See also military search

***military search**

(DOD) The management and application of systematic procedures and appropriate detection equipment to locate specified targets.

neutralize

(DOD) 1. As pertains to military operations, to render ineffective or unusable. 2. To render enemy personnel or material incapable of interfering with a particular operation. 3. To render safe mines, bombs, missiles, and booby traps. 4. To make harmless anything contaminated with a chemical agent (JP 1-02).

Render-safe procedures

(DOD) Those particular courses or modes of action taken by explosive ordnance personnel for access to, diagnosis, rendering safe, recovery, and final disposal of explosive ordnance or any hazardous material associated with an explosive ordnance incident. The explosive ordnance procedures involving the application of special explosive ordnance methods and tools to provide for the interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation (JP 1-02).

system

A system is a set of different elements so connected or related as to perform a unique function not performable by the elements or components alone.

unexploded explosive ordnance; unexploded ordnance

(DOD) Explosive ordnance which has been primed, fused, armed, or otherwise prepared for action, and which has been fired, dropped, launched, projected, or placed in such a manner as to constitute a hazard to operations, installations, personnel, or material and remains unexploded either by malfunction or design or for any other cause. Also called UXO (JP 1-02).

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

ARMY PUBLICATIONS

FM 1-02. *Operational Terms and Graphics.* MCRP 5-12A. 21 September 2004.

FM 2-0. *Intelligence.* 17 May 2004.

FM 3-34. *Engineer Operations.* 2 January 2004.

FM 3-90. *Tactics.* 4 July 2001.

FM 3-100.12. *Risk Management for Multiservices Tactics, Techniques, and Procedures.* MCRP 5-12.1C/NTTP 5-03.5/ AFTTP(1) 3-2.34. 15 February 2001.

FM 3-100.38. *(UXO) Multiservice Procedures for Unexploded Ordnance in a Joint Environment.* MCRP 3-17.2B/NTTP 3-02.4.1 (Rev A)/AFTTP (1) 3-2.12. 23 August 2001.

FM 4-30.5. *Explosive Ordnance Disposal Operations.* 28 April 2005.

FM 5-0. *Army Planning and Orders Production.* 20 January 2005.

FM 5-116. *Engineer Operations: Echelons Above Corps.* 9 February 1999. (Will be revised as FM 3-34.211.)

FM 6-20-10. *Tactics, Techniques, and Procedures for the Targeting Process.* MCRP 3-1.6.14. 8 May 1996.

FM 7-92. *The Infantry Reconnaissance Platoon and Squad (Airborne, Air Assault, Light Infantry).* 23 December 1992.

FM 7-100. *Opposing Force Doctrinal Framework and Strategy.* 1 May 2003.

FM 20-32. *Mine/Countermine Operations.* 29 May 1998. (Will be revised as FM 3-34.210.)

FM 21-16/MCWP 3-17.3. *Unexploded Ordnance (UXO) Procedures.* FMFM 13-8-1. 30 August 1994. (Will be revised as FM 4-30.11.)

FM 34-130. *Intelligence Preparation of the Battlefield.* 8 July 1994. (Will be revised as FM 2-01.3.)

FM 90-7. *Combined Arms Obstacle Integration.* 29 September 1994. (Will be revised as FM 3-90.13.)

FM 100-14. *Risk Management.* 23 April 1998.

FMI 4-30.5. *Modular EOD Operations.*

GTA 09-12-001. *Unexploded Ordnance Procedures (UXO).* 3 January 1992.

GTA 90-01-001. *Improvised Explosive Device(IED) and Vehicular Borne Improvised Explosive Device (VBIED) Smart Card.* 20 May 2004.

ST 2-50. *Intelligence and Electronic Warfare (IEW) Systems.* 1 June 2002.

ST 2-01.301. *Specific TTP for Application of Intelligence Preparation of the Battlefield.* To be published within six months.

ST 2-22.7. *Tactical Human Intelligence and Counterintelligence Operations.* 1 April 2002.

ST 20-23-10. *Use of Specialized Search Dogs in Military Operations.* February 2004.

TC 9-21-01. *(O) Soldiers Improvised Explosive Device (IED) Awareness Guide Iraq and Afghanistan Theaters of Operation.* 28 May 2004.

TC 20-32-5, *Commander's Reference Guide for Land Mine and Explosive Hazards (Iraq).* 13 February 2003.

JOINT PUBLICATIONS

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 12 April 2001.

JP 3-34. *Engineer Doctrine for Joint Operations.* 5 July 2000.

JP 4-04. *Joint Doctrine for Civil Engineering Support.* 27 September 2001.

MISCELLANEOUS

Army Campaign Plan

Joint Vision 2020. June 2000.

STANDARDIZATION AGREEMENTS

STANAG 2221 (EOD). *Explosive Ordnance Disposal Reports and Messages-AEODP-6 February-2001.* 1 June 2001.

STANAG 2237 (ENGR). *Obstacle Numbering.*

STANAG 2283. *Military Search* (Draft).

STANAG 2430 (ENGR). *Land Forces Combat Engineer Messages, Reports and Returns (R2) – AengrP-2(B).* 18 August 2004.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication. The asterisk denotes that this source was also used to develop this publication.

ARMY PUBLICATIONS

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

*FM 1-02. *Operational Terms and Graphics.* MCRP 5-12A. 21 September 04.

*FM 2-0. *Intelligence.* 17 May 2004.

*FM 3-34. *Engineer Operations.* 2 January 2004.

*FM 3-90. *Tactics.* 4 July 2001.

*FM 3-100.12. *Risk Management for Multiservices Tactics, Techniques, and Procedures.* MCRP 5-12.1C/NTTP 5-03.5/ AFTTP(1) 3-2.34. 15 February 2001.

*FM 3-100.38. *(UXO) Multiservice Procedures for Unexploded Ordnance in a Joint Environment.* MCRP 3-17.2B/NTTP 3-02.4.1 (Rev A)/AFTTP (1) 3-2.12. 23 August 2001.

*FM 4-30.5. *Explosive Ordnance Disposal Operations.* 28 April 2005.

*FM 5-0. *Army Planning and Orders Production.* 20 January 2005.

*FM 5-116. *Engineer Operations: Echelons Above Corps.* 9 February 1999. (Will be revised as FM 3-34.211.)

*FM 6-20-10. *Tactics, Techniques, and Procedures for the Targeting Process.* MCRP 3-1.6.14. 8 May 1996.

*FM 7-92. *The Infantry Reconnaissance Platoon and Squad (Airborne, Air Assault, Light Infantry).* 23 December 1992.

*FM 7-100. *Opposing Force Doctrinal Framework and Strategy.* 1 May 2003.

*FM 20-32. *Mine/Countermine Operations.* 29 May 1998. (Will be revised as FM 3-34.210.)

*FM 21-16/MCWP 3-17.3. *Unexploded Ordnance (UXO) Procedures.* FMFM 13-8-1. 30 August 1994. (Will be revised as FM 4-30.11.)

*FM 34-130. *Intelligence Preparation of the Battlefield.* 8 July 1994. (Will be revised as FM 2-01.3.)

*FM 90-7. *Combined Arms Obstacle Integration.* 29 September 1994. (Will be revised as FM 3-90.13.)

*FM 100-14. *Risk Management.* 23 April 1998.

*FMI 4-30.5. *Modular EOD Operations.*

*GTA 09-12-001. *Unexploded Ordnance Procedures (UXO).* 3 January 1992.

*GTA 90-01-001. *Improvised Explosive Device(IED) and Vehicular Borne Improvised Explosive Device (VBIED) Smart Card.* 20 May 2004.

*ST 2-50. *Intelligence and Electronic Warfare (IEW) Systems.* 1 June 2002.

*ST 2-01.301. *Specific TTP for Application of Intelligence Preparation of the Battlefield.* To be published within six months.

*ST 2-22.7. *Tactical Human Intelligence and Counterintelligence Operations.* 1 April 2002.

*ST 20-23-10. *Use of Specialized Search Dogs in Military Operations.* February 2004.

*TC 9-21-01. *(O) Soldiers Improvised Explosive Device (IED) Awareness Guide Iraq and Afghanistan Theaters of Operation.* 28 May 2004.

*TC 20-32-5, *Commander's Reference Guide for Land Mine and Explosive Hazards (Iraq).* 13 February 2003.

JOINT PUBLICATIONS

*JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 12 April 2001.

*JP 3-34. *Engineer Doctrine for Joint Operations.* 5 July 2000.

*JP 4-04. *Joint Doctrine for Civil Engineering Support.* 27 September 2001.

MISCELLANEOUS

**Army Campaign Plan*

**Joint Vision 2020.* June 2000.

STANDARDIZATION AGREEMENTS

*STANAG 2221 (EOD). *Explosive Ordnance Disposal Reports and Messages-AEODP-6 February-2001.* 1 June 2001.

*STANAG 2237 (ENGR). *Obstacle Numbering.*

*STANAG 2283. *Military Search* (Draft).

*STANAG 2430 (ENGR). *Land Forces Combat Engineer Messages, Reports and Returns (R2) – AengrP-2(B).* 18 August 2004.

READINGS RECOMMENDED

These sources contain relevant supplemental information.

AR 40-10. *Health Hazard Assessment Program in Support of the Army Materiel Acquisition Decision Process.* 1 October 1991.

AR 385-10. *The Army Safety Program.* 29 February 2000.

AR 385-16. *System Safety Engineering and Management.* 2 November 2001.

AR 385-63. *Range Safety.* 19 May 2003.

AR 385-64. *U.S. Army Explosives Safety Program.* 1 February 2000.

DA Pam 350-38. *Standards in Weapons Training.* 1 October 2002.

DA Pam 385-64. *Ammunition and Explosives Safety Standards.* 1 February 2000.

DOD 6055.9-STD. *DOD Ammunition and Explosives Safety Standards.* October 2004.

FM 3-0. *Operations.* 14 June 2001.

FM 3-06. *Urban Operations.* 1 June 2003.

FM 3-06.11. *Combined Arms Operations in Urban Terrain.* 28 February 2002.

FM 3-34.2. *Combined-Arms Breaching Operations.* 31 August 2000. (Will be revised as FM 3-90.11.)

FM 3-34.230. *Topographic Operations.* 3 August 2000.

FM 5-10. *Combat Engineer Platoon.* 3 October 1995.

FM 5-34. *Engineer Field Data.* 30 August 1999. (Will be revised as FM 3-34.310.)

FM 5-170. *Engineer Reconnaissance.* 5 May 1998.

FM 5-250. *Explosives and Demolitions.* 30 July 1998. (Will be revised as FM 3-34.214.)

FM 101-5-2. *U.S. Army Report and Message Formats.* 29 June 1999. (Will be revised as FM 6-99.2.)

IMAS 08.40. *Marking Mine and UXO Hazards. Second Edition 2.* 1 January 2003.

JP 3-34. *Engineer Doctrine for Joint Operations.* 5 July 2000.

MIL-STD-882C (Revision). *System Safety Program Requirements.* 19 January 1993.

STANAG 2002 (NBC). *Warning Signs for the Marking of Contaminated or Dangerous Land Areas, Complete Equipments, Supplies, and Stores.* 21 May 2003.

STANAG 2014. *Formats for Orders and Designation of Timings, Locations, and Boundaries.* 17 October 2000.

STANAG 2036 (ENGR)/QSTAG 518. *Land Mine Laying, Marking, Recording and Reporting Procedures.* 27 January 2005.

STP 5-12B1-SM. *Soldier's Manual: MOS 12B, Combat Engineer, Skill Level 1.* 31 August 2000.

TM 43-0001-36. *Army Ammunition Data Sheets for Land Mines (FSC 1345).* 1 September 1994.

FMI 3-34.119/MCIP 3-17.01
21 September 2005
Expires 21 September 2007

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

SANDRA R. RILEY
Administrative Assistant to the
Secretary of the Army
0525731

DISTRIBUTION:

Active Army, Army National Guard, and US Army Reserve: Not to be distributed. Electronic media only.

By Direction of the Commandant of the Marine Corps:

J. N. MATTIS
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development

Marine Corps PCN: 146 000003 00

PIN: 082769-000